



SECURING THE NEXT RIPPLE IN INFORMATION SECURITY:

THE DEFENSE INDUSTRIAL BASE (DIB)

GRADUATE RESEARCH PROJECT

Justin W. Swartzmiller, Major, USAF

AFIT/ICW/ENV/12-J02

**DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY**

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION UNLIMITED.

The views expressed in this report are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government. This material is declared a work of the United States Government and is not subject to copyright protection in the United States.

AFIT/ICW/ENV/12-J02

SECURING THE NEXT RIPPLE IN INFORMATION SECURITY:
THE DEFENSE INDUSTRIAL BASE (DIB)

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the
Degree of Master of Science in Cyber Warfare

Justin W. Swartzmiller

Major, USAF

June 2012

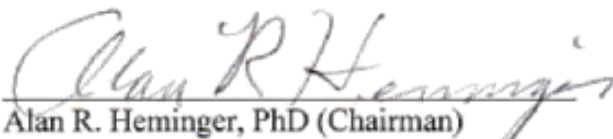
DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION UNLIMITED.

SECURING THE NEXT RIPPLE IN INFORMATION SECURITY:
THE DEFENSE INDUSTRIAL BASE (DIB)

Justin W. Swartzmiller

Major, USAF

Approved:


Alan R. Heminger, PhD (Chairman)

4 Jun 12
Date


Robert F. Mills, PhD (Member)

30 MAY 12
Date


Michael R. Grimala, PhD, CISM, CISSP (Member)

30 May 12
Date

Abstract

America's one-time technological advantage is gone; much of its intellectual property secrets have been stolen. For sometime, our adversaries have been attacking the Department of Defense's (DoD) networks to obtain any sensitive information. Recently, attackers have expanded their attacking efforts, to include the Defense Industrial Base (DIB), due to DoD's increased network defenses. This research will answer the core issue of how to secure sensitive information within the DIB and determine if a Cybersecurity Maturity Model can be utilized to assess the level of security the DIB provides to sensitive unclassified DoD information.

An initial Literature Review was conducted and the findings were used to develop a maturity model that may be used to enhance cybersecurity within the DIB. Next, a Delphi study was conducted to evaluate the proposed Cybersecurity Maturity Model methodology using four criteria: comprehensiveness, accuracy, completeness, and usefulness. The Delphi committee consisted of representatives from both the DoD and private sector; with each member's experience characterized as computer network attack, computer network exploitation or computer network defense.

The findings of the Delphi committee support that a Cybersecurity Maturity Model can be developed successfully to better focus the DIB's efforts and demonstrate an organizations cyber security capability.

Dedication

To My Family

Acknowledgments

I would like to convey my heartfelt appreciation to the members who volunteered to be part of the Delphi panel. Their candid comments, recommendations and most importantly their time are very much valued. I would like to thank my research advisor, Dr. Alan Heminger, for his patience and direction while conducting this research. I would like to thank my sponsor, Mr. Steven D. Shirley, SES, from the DoD Cyber Crime Center (DC3), for his keenness and offering his staff's time and expertise on occasion, specifically Mr. Patrick Dempsey. I would also like to thank my daughter and son. Although, I could not attend all of their social events, they provided me with their understanding, support and a well-deserved break from time to time. Finally, I would like to especially thank my lovely wife, whom has supported me through numerous deployments, TDY's, and PCS moves; I love you and look forward to our next adventure.

Justin Swartzmiller

Table of Contents

	Page
Abstract.....	iv
Dedication.....	v
Acknowledgments.....	vi
Table of Contents.....	vii
List of Figures	ix
List of Tables	x
List of Acronyms	xi
I. Introduction	1
1.1 Introduction.....	1
1.2 Definitions of Key Terms	2
1.3 Issue: How to secure the DIB to stem Cyberspace losses	4
1.4 Implications of the status quo	6
1.5 Scope.....	7
1.6 Research Question	8
1.7 Research Approach.....	8
II. Literature Review	9
2.1 The Awakening.....	9
2.2 Case for Action	14
2.3 Project 12 Report	15
2.4 Cyberspace Policy Review	17
2.5 The Comprehensive National Cybersecurity Initiative (CNCI)	19
2.6 International Strategy for Cyberspace	20
2.7 DoD Strategy for Operating in Cyberspace.....	21
2.8 DIB Cyber Security/Information Assurance (CS/IA) Partnership	23
2.9 Joint Cybersecurity Services Pilot (JCSP).....	24
2.10 Capability Maturity Models.....	26
2.11 Reference Engineering Framework Defined	30
2.12 A Proposed Cybersecurity Maturity Model.....	31

	Page
III. Research Methodology.....	33
3.1 Introduction.....	33
3.2 Overview of Methodology.....	34
3.3 The Delphi Method.....	34
3.4 Phase I: Cyberspace Security Model Development.....	36
3.4.1 Model Research	36
3.4.2 Model Development	37
3.4.3 Questionnaire Development	42
3.4.4 The Study Population	43
3.4.5 The Delphi Panel Participants	44
3.5 Phase II: Model Evaluation and Validation.....	46
3.5.1 Round One	46
3.5.2 Round Two	47
3.6 Phase III: Analysis of Delphi Study Results, Model Modification and Recommendations for Future Research	48
IV. Results and Analysis	49
4.1 Overview.....	49
4.2 Summary of Results.....	49
4.3 Evaluating the Model.....	53
4.4 Research Results	59
V. Discussion & Recommendations.....	62
5.1 Conclusion	62
5.2 Recommendations for Future Research.....	63
5.3 Closing Thought	63
Appendix A - Delphi Group Primer.....	65
Appendix B – Proposed Cybersecurity Model Round One	68
Appendix D - Delphi Group Instructions Round Two.....	74
Appendix E - Modified Cybersecurity Model Round Two	75
Appendix F - Delphi Questionnaire Round Two	79
Bibliography	87
Vita	90

List of Figures

Figure	Page
1. Community Cyber Security Maturity Model.....	39

List of Tables

Table	Page
1. Military Critical Technology List (1996)	11
2. CNCI Initiatives	19
3. Area of Expertise	45
4. Breakdown by Organizational Area.....	45
5. Breakdown by Functional Area	45

List of Acronyms

CCSMM- Community Cyber Security Maturity Model

CDC- Cleared Defense Contractor

CERT-REF- Computer Emergency Response Team- Resilience Engineering Framework

CERT-RMM- Computer Emergency Response Team- Resilience Management Model

CI- Counterintelligence

CIA-Central Intelligence Agency

CIKR- Critical Infrastructure and Key Resources

CMM- Capability Maturity Model

CMMI- Capability Maturity Model Integration

CMU- Carnegie Mellon University

CNCI- Comprehensive National Cybersecurity Initiative

CS/IA- Cyber Security/Information Assurance

CSP- Commercial Service Provider

DCISE- DoD-DIB Collaborative Information Sharing Environment

DIA- Defense Intelligence Agency

DIB- Defense Industrial Base

DIBNet-S – Defense Industrial Base Network-Secure

DIS- Defense Investigative Service

DoD- Department of Defense

DOE- Department of Energy

DSS- Defense Security Service

FBI- Federal Bureau of Investigation

I SAC- Information Sharing and Analysis Centers

ISO- Information Sharing Organizations

IT-Information Technology

JCSP- Joint Cybersecurity Services Pilot

NACIC- National Counterintelligence Center

NASA- National Aeronautics and Space Administration

NCC- National Coordinating Center

NIPP- National Infrastructure Protection Plan

NISP-National Industrial Security Program

NSA- National Security Agency

NSPD-54/HSPD-23- National Security Presidential Directive 54/Homeland Security

Presidential Directive 23

ODNI- Office of the Director of National Intelligence

PARS- Published Appraisal Results

R&D-Research and Development

SCAMPI- Standard CMMI Appraisal Method for Process Improvement

SEI- Software Engineering Institute

US-CERT- US Computer Emergency Readiness Team

I. Introduction

“What we have witnessed over the past five to six years has been nothing short of a historically unprecedented transfer of wealth — closely guarded national secrets (including from classified government networks), source code, bug databases, email archives, negotiation plans and exploration details for new oil and gas field auctions, document stores, legal contracts, SCADA configurations, design schematics and much more has “fallen off the truck” of numerous, mostly Western companies and disappeared in the ever-growing electronic archives of dogged adversaries.”

—Revealed: Operation Shady RAT, White Paper, Dmitri Alperovitch (2011)

1.1 Introduction

“America’s one-time technological advantage is gone; much of its intellectual property secrets have been stolen. Global cyber crime is now more profitable than the drug trade.” These two statements summarize what the speakers at the Air Force Association cyber-conference held in March 2012 reported (Ewing 2012). For sometime, it has been quite clear that our adversaries have been attacking the Department of Defense’s (DoD) networks to obtain any and all sensitive information they could.

In recent years as the DoD has increased its network defenses a shift has occurred. The attackers, although still attacking the DoD, have expanded their attacking efforts to include the Defense Industrial Base (DIB) and even beyond to mainstream American companies, those companies not currently associated with the DoD. Attackers have also become more focused. In fact, Richard Bejtlich, chief security officer for the info-

security firm Mandiant, said during the 2012 Air Force Association cyber-conference “many attackers don’t even bother with the wholesale vacuuming of information that used to characterize cyber-snooping. Now hackers go after very specific pieces of information.” The DoD and DIB needs to leverage any and all measures it can to secure their sensitive information. Especially in the research and development (R&D) realm as new innovations are created, they need to be protected. This research paper will answer the core issue of how to secure sensitive information within the DIB and determine if a Cybersecurity Maturity Model can be utilized to assess the level of security the DIB provides to sensitive unclassified DoD information.

1.2 Definitions of Key Terms

A Cleared Defense Contractor is defined as a company or other designated entity in private industry or at a college/university that has access to U.S. classified information and participates in the National Industrial Security Program (NISP); the entity must have a legitimate U.S. Government or foreign government requirement for such access (DoD 2011, NISP Fact Sheet).

Cyberspace is the interdependent network of information technology (IT) infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. This definition appears in the *Cyberspace Policy Review* (Obama 2009) however, the document attributes that the definition originates in the classified National Security Presidential Directive 54/Homeland Security Presidential Directive 23 issued by President George W. Bush in January 2008.

Defense Industrial Base (DIB) is defined as “The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements” (JP-1-02, 106).

Economic espionage occurs when an actor, knowing or intending that his or her actions will benefit any foreign government, instrumentality or agent, knowingly: (1) steals, or without authorization appropriates, carries away, conceals, or obtains by deception or fraud a trade secret; (2) copies, duplicates, reproduces, destroys, uploads, downloads, or transmits that trade secret without authorization; or (3) receives a trade secret knowing that the trade secret had been stolen, appropriated, obtained or converted without authorization (18 USC § 1831 January 2012).

Industrial espionage or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner by: (1) stealing, or without authorization appropriating, carrying away, concealing, or obtaining by deception or fraud information related to that secret; (2) copying, duplicating, reproducing, destroying, uploading, downloading, or otherwise transmitting that information without authorization; or (3) receiving that information knowing that that information had been stolen, appropriated, obtained or converted without authorization (18 USC § 1832 January 2012).

Intellectual Property is an intangible property, such as an idea or an invention; creations of a person's intellect. "Just as the U.S. law grants ownership rights over material possessions, such as a home or a bicycle, it similarly grants individuals legal rights over intangible property, such as an idea or an invention. When a person creates something that is novel and unique, the law recognizes its value and grants the creator the respect and integrity of ownership for this intellectual property. Intellectual property's diversity is reflected in four distinct areas of law that protect it: copyrights, trademarks, trade secrets, and patents." (Department of Justice 2004)

Sensitive is defined as "information or technology (a) that has been classified or controlled by a US Government organization or restricted in a proprietary manner by a US corporation or other institution, or (b) that has or may reasonably be expected to have military, intelligence, or other uses with implications for US national security, or (c) that may enhance the economic competitiveness of US firms in global markets" (Office of National Counterintelligence Executive 2011).

1.3 Issue: How to secure the DIB to stem Cyberspace losses

Dmitri Alperovitch, the vice president of threat research for McAfee, released a report in 2011 entitled Operation Shady Rat in which he stated, "I am convinced that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly), with the great majority of the victims rarely discovering the intrusion or its impact. In fact, I divide the entire set of Fortune Global 2000 firms into two categories: those that *know they've been compromised* and those that *don't yet know*." This notion is

very troubling because some companies may never realize they are compromised and ultimately hurt themselves and those companies they do business with.

Couple Mr. Aplerovitch's statement with recent statements from a Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, "that the U.S. intelligence community has improved its collaboration to better address cyber espionage in the military and national-security areas. Yet today's legislative framework severely restricts us from fully addressing domestic economic espionage." and "Corporate America must do its part, too. If we are to ever understand the extent of cyber espionage, companies must be more open and aggressive about identifying, acknowledging and reporting incidents of cyber theft. Companies must also invest more in enhancing their employees' cyber skills; it is shocking how many cyber-security breaches result from simple human error such as coding mistakes or lost discs and laptops" (McConnell, Chertoff, Lynn 2012).

These statements imply that we have greatly improved our activities in dealing with cyber espionage although it appears to be solely in the military realm. The U.S. is severely hindered on the domestic side due to restrictions and/or authorities. Furthermore, the corporate side must step-up their efforts to identify and report all cyber incidents. These limitations, by extension, are severely affecting the DIB, as a significant portion (the DIB minus DoD) of the DIB is made up the "domestic" and "corporate" portions of the U.S.

1.4 Implications of the status quo

“Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will continue at a high level and will represent a growing and persistent threat to US economic security. The nature of the cyber threat will evolve with continuing technological advances in the global information environment. The trend in both commercial and government organizations toward the pooling of information processing and storage will present even greater challenges to preserving the security and integrity of sensitive information.” (Office of the National Counterintelligence Executive (2011).

As stated earlier the DoD understood and took action to harden its networks through collaboration which allowed them to better address cyber espionage. The DoD also realized the adage “a chain is only as strong as its weakest link”, meaning although the DoD networks were becoming more secure they could still be losing DoD sensitive information through other means. For instance, if their DIB partners do not also harden their networks they could become an easier yet just as fruitful target for an adversary.

To address this shortfall, the DoD established the DIB CS/IA (Cyber Security/ Information Assurance) Program to enable information sharing between industry partners and the U.S. Government. “The goal of this program is to protect sensitive unclassified DoD program and technology information resident on, or transiting, DIB unclassified networks. To participate in the DIB CS/IA partners must:

- Be a Cleared Defense Contractor (CDC) with a Facility Clearance granted by Defense Security Service (DSS)
- Have cleared employees (Secret clearance required) empowered to direct and/or support the program on behalf of the company
- Have DoD-approved medium assurance External Certificate Authority certificates
- Have or obtain a COMSEC account
- Obtain DIBNet-S (Defense Industrial Base Network-Secure) for classified communications
- Sign a bilateral framework agreement with DoD” (DoD 2012, DIB CS/IA)

“The Defense Security Service (DSS) administers the NISP on behalf of the Department of Defense as well as 24 non-DoD federal agencies within the Executive Branch. Presently, DSS has Industrial Security oversight responsibility for over 13,300 cleared companies participating in the NISP” (DoD 2011, NISP Fact Sheet).

As the DIB/CA continues their information sharing activities, other efforts to aid the DIB may enhance their security of DoD sensitive information and ensure continuous improvement.

1.5 Scope

This research effort will focus on developing and assessing a maturity model for cyberspace security, specifically protecting sensitive information within the DIB, which can be used to assess the status and capability obtained per identified process.

The scope of this research paper is to identify and review existing cyberspace policies, strategies, initiatives and maturity models or frameworks (to include those

in information security and cyberspace security); then develop, propose and assess a maturity model that will focus on identifying processes that enhance securing sensitive information within the DIB.

1.6 Research Question

The research question for this study is: can a Cybersecurity Maturity Model be utilized to assess the level of security the DIB provides to sensitive unclassified DoD information?

1.7 Research Approach

The research methodology chosen for this research effort is a Delphi study. A review of existing information security and cyberspace security maturity models/frameworks will be performed; with the intent of identifying aspects/processes that can be applied specifically to a cyberspace framework, which may in turn be utilized to support cyber security within the DIB. The researcher will develop and propose a cyberspace maturity model that 1) provides a common model for improvement of securing sensitive information 2) provides a means for assessing the status and progress of the identified processes in securing sensitive information and 3) provides a means for comparison across the DIB to a Delphi study panel. The Delphi panel will identify and assess the processes that will be included in the initial framework, identify and propose modifications to the initial framework and provide favorable comments for those processes that should remain in the framework as presented to the Delphi panel.

II. Literature Review

“The user's going to pick dancing pigs over security every time.” Bruce Schneier

This chapter summarizes the literature that was reviewed in developing a starting point for answering the guiding research question. In order to achieve the goal of determining if a maturity model can be utilized to assess the level of cybersecurity in which a DIB contractor provides to sensitive unclassified DoD information; it is important to provide a sense for how severe the loss of sensitive information is to National Security. To accomplish this, a review was done to determine how important the U.S. Government values its information, and the steps they have taken to protect it. Additionally, an assessment was completed on maturity models, to include Information Security and Cybersecurity, Capability Maturity Models, and the CERT-Resilience Management Model.

2.1 The Awakening

In 1995 the U.S. Congress passed the *Intelligence Authorization Act for Fiscal Year 1995* which requires that the President provide a report to the Congress, on foreign industrial espionage targeted against U.S. industry. This report is prepared by the National Counterintelligence Center on an annual basis. The *Act* required that the report address four issues:

- The respective policy functions and operational roles of the agencies of the Executive Branch of the Federal Government in identifying and countering threats to U.S. industry of foreign industrial espionage, including the manner in which such functions and roles are coordinated

- The means by which the Federal Government communicates information on such threats, and on methods to protect against such threats, to US industry in general and to US companies known to be targets of foreign espionage
- The specific measures that are being or could be undertaken in order to improve the activities referred to in the above paragraphs, including proposals for any modifications of law necessary to facilitate the undertaking of such activities
- The threat to US industry of foreign industrial espionage and any trends in that threat (National Counterintelligence Center, 1995)

The inaugural 1995 report laid out the policy functions and operational roles for the numerous agencies within the U.S. Government that would communicate information on [industrial espionage] threats, and on methods to protect against such threats, to U.S. industry in general and to U.S. companies known to be targets of foreign espionage. The agencies included: Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), Defense Investigative Service (DIS), Department of Defense (DoD), Military Services (Air Force Office of Special Investigations and Naval Criminal Investigative Service), Department of Energy (DOE), Federal Bureau of Investigation (FBI), National Counterintelligence Center (NACIC), National Aeronautics and Space Administration (NASA), and National Security Agency (NSA). Specifically the DIA, DIS, DoD and Military Services would share information with DoD contractors.

The Annual Report to Congress on Foreign Economic Collection and Industrial Espionage: 1996 stated, “according to the FBI and DIS, high-technology and defense related industries remain the primary targets of foreign economic intelligence collection operations. The most likely industry targets of economic espionage and other collection

activities during the past year include the following areas, most of which are included on the 1996 Military Critical Technology List, see table 1.

Table 1 Military Critical Technology List (1996)

Advanced materials and coatings	Information systems
Advanced transportation & engine technology	Information warfare
Aeronautics systems	Manufacturing and fabrication
Aerospace	Manufacturing processes
Armaments and energetic materials	Marine systems
Biotechnology	Materials
Chemical and biological systems	Nuclear systems
Computer software and hardware	Semiconductors
Defense and armaments technology	Sensors and lasers
Directed and kinetic energy systems	Signature control
Electronics	Space systems
Energy research	Telecommunications
Guidance, navigation & vehicle control	Weapons effects and countermeasures

The report went on to say “because of the growing popularity and expansion of the Internet, the US defense industry reports significant increases in security countermeasures incidents associated with computer-based collection attempts. Large amounts of DoD technical information are transferred over the Internet on a daily basis and could be targeted by hostile entities” (National Counterintelligence Center 1996). This report recognized and documented the concern that an adversary could interrupt or obtain DoD sensitive information.

In 2001, the Annual Report to Congress on Foreign Economic Collection and Industrial Espionage added a new category, Internet Activity (Cyber Attack and Exploitation). “This category addressed cyber attack and exploitation vice Internet-based requests for information. The majority of Internet endeavors were foreign probes searching for potential weaknesses in systems for exploitation. One example was a network attack that, over the period of a day, involved several hundred attempts to use multiple passwords to illegally obtain access to a cleared defense facility’s network. This example reflects the extent to which intelligence collectors are attempting to use the Internet to gain access to sensitive or proprietary information. Given the considerable effort that is under way in the cyber attack and exploitation arenas, substantial resources will need to be allocated in the future to ensure adequate security countermeasures” (National Counterintelligence Center 2001).

The overall concern remained constant with no appreciable threat, as documented in the 2001-2004 annual reports to Congress. However, the 2005 report included a significant departure statement from previous years. “The Counterintelligence (CI) Community is unanimous in the view that the illegal outflow of technology imposed huge costs on the United States. A sample of the types of technologies lost during the year indicates the potential extent of damage. Recent losses have hurt the United States by:

- Enabling foreign militaries to leapfrog technological hurdles and to acquire sophisticated capabilities that might have otherwise taken years to develop. A former Department of Defense (DoD) contractor provided China and a number of other countries with access to classified and export-controlled infrared signature

suppression technologies developed for the B-2 Stealth Bomber. Such acquisitions would provide foreign militaries with an invaluable jump in developing stealth aircraft of their own or in countering the US advantage. Making it possible for foreign firms to gain a competitive economic edge over US competitors, thereby undermining the US economy.

- As in years past, entities from a relatively small number of countries accounted for the majority of foreign targeting of US technologies in FY 2005. China and Russia are two of the most aggressive collectors. The major collectors have been repeatedly identified targeting multiple US Government organizations and all types of technologies since at least 1997, when the CI Community first began systematically reporting on targeting efforts” (National Counterintelligence Center 2005).

This timeframe (early to mid 2000’s) is when the U.S. concerns’ became reality. The increased connectivity around the world combined with the drive to digitize work environments drove countries to be more efficient; but the connectivity created an unforeseen side effect—a cyber watershed. The downside to the digitization of records is security. It is much harder for most people to think about electronic (cyber) security than it is physical security. Adversaries started to take advantage of the lack of cyber security to steal data, to include sensitive data. This turned out to be much easier and cheaper than the old ways of physically stealing documents plus it provided many additional benefits such as: speed, difficult to attribute who had stolen the data, could help close technological gaps and others.

2.2 Case for Action

“Dating back to 2005 U.S. officials and cyber-security experts has said Chinese Web sites were involved in several of the biggest attacks, including some at the country's nuclear-energy labs and large defense contractors. There has also been a string of attacks on networks at the State, Commerce, Defense and Homeland Security departments in the past year and a half” (implying 2006-2007) (Nakashima 2008).

To protect against a rising number of attacks on federal agencies' computer systems President George W. Bush, took action and expanded the intelligence community's role in monitoring Internet traffic. On January 8, 2008 he signed a classified joint directive called the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). “The directive formalized a series of continuous efforts designed to further safeguard Federal Government systems and reduce potential vulnerabilities, protect against intrusion attempts, and better anticipate future threats (DHS Fact Sheet 2008).” The directive also “expanded the NSA's role in cyber-security. Previous to this directive, the government's efforts to protect itself from cyber-attacks -- which run the gamut from hackers to organized crime to foreign governments trying to steal sensitive data – were conducted in a piecemeal fashion. Under the new initiative, a task force headed by the Office of the Director of National Intelligence (ODNI) was tasked to coordinate efforts in identifying the source of cyber-attacks against government computer systems. As part of that effort, the Department of Homeland Security worked to protect the systems and the Pentagon was asked to devise strategies for counterattacks against the intruders” (Nakashima 2008).

2.3 Project 12 Report

The NSPD-54/HSPD-23 further “directed the Secretary of Homeland Security, in consultation with the heads of other Sector-Specific Agencies, to submit a report detailing the policy and resource requirements for improving the protection of privately owned U.S. critical infrastructure networks. The Project 12 Report was required to detail how the U.S. Government can partner with the private sector to leverage investment in intrusion protection capabilities and technology, increase awareness about the extent and severity of cyber threats facing critical infrastructure, enhance real-time cyber situational awareness, and encourage intrusion protection for critical information technology infrastructure (DHS Project 12, 2008).”

The report provided many recommendations to provide a path to improve U.S. critical infrastructure and key resources (CIKR) cybersecurity. “A combination of planning and pilot programs is intended to build confidence over time and to allow course corrections to change with the dynamic cyber environment. The recommendations included:

- Develop a plan to identify specific goals and outcome metrics related to securing CIKR sector networks
- Promote current public-private cyber information sharing efforts via the National Infrastructure Protection Plan (NIPP) Framework by fostering trust through consistent and timely communications and consensus building
- Develop a plan using the NIPP Partnership Framework to include the CIKR sectors into ongoing Comprehensive National Cybersecurity Initiative (CNCI) efforts
- Leverage existing frameworks to develop, as appropriate, new vehicles, rules, and instruments between public and private sectors to improve sharing of actionable cyber information

- Scope the requirements for implementing real-time cyber situational awareness
- Evaluate the feasibility of sharing Federally developed technology capabilities with CIKR
- Expedite the TS/SCI clearance process for appropriate private-sector representatives for when "tear-line" unclassified cybersecurity documents are not available
- Enhance information sharing and analysis organizations, whether information sharing and analysis centers (ISAC) or other information sharing organizations (ISO), to make them the focal point of cyber operational activity with the 18 CIKR sectors
- Enhance information sharing mechanisms to provide an environment in which technological barriers do not impede cyber information sharing processes
- Expand US-Computer Emergency Readiness Team (US-CERT) National Coordinating Center for Telecommunications (NCC) joint operational capabilities to include private sector CIKR participation to enhance CIKR real-time situational awareness
- Establish a mechanism to give companies opportunities and incentives to invest in R&D and-based on legal, security, and investment-level criteria-potentially allow companies to obtain intellectual property rights to the results of government-funded or government-partnered cybersecurity R&D
- Investigate new ways to drive improvement in the cybersecurity posture within the private sector in those cases where market forces yield an insufficient value proposition
- Investigate methods to encourage cybersecurity across the business community nationwide similar to those used within private-sector CIKR” (DHS Project 12, 2008).”

This report represented a new level of cooperation between the federal government and industry plus it helped identify gaps in cybersecurity and information sharing.

2.4 Cyberspace Policy Review

“President Obama identified cybersecurity as one of the most serious economic and national security challenges we face as a nation. Shortly after taking office, the President therefore ordered a thorough review of federal efforts to defend the U.S. information and communications infrastructure and the development of a comprehensive approach to securing America’s digital infrastructure (Obama Cyberspace Policy Review 2009)”.

In testimony before the Senate Armed Services Committee in March 2009, the Director of National Intelligence, Dennis Blair stated: “As government, private sector, and personal activities continue to move to networked operations, as our digital systems add ever more capabilities, as wireless systems become even more ubiquitous and as the design, manufacture, and service of information technology have moved overseas, the threat will continue to grow. A growing array of state and non-state adversaries are increasingly targeting—for exploitation and potentially disruption or destruction—our information infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious.”

In early 2009, “the President directed a 60-day, comprehensive, “clean-slate” review to assess U.S. policies and structures for cybersecurity. Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and

activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure” (Obama Cyberspace Policy Review 2009).

The review points out that “the digital infrastructure’s architecture was driven more by considerations of interoperability and efficiency than of security. Consequently, a growing array of state and non-state actors are compromising, stealing, changing, or destroying information and could cause critical disruptions to U.S. systems.”

The review further found there was a need for greater coordination and integrated development of policy. The review developed findings and options for action under five key topics: (1) leading from the top, (2) building capacity for a digital nation, (3) sharing responsibility for cybersecurity, (4) improving information sharing and incident response, and (5) building the architecture of the future. It is under the third key topic, sharing the responsibility for cybersecurity, that the review recommends improving the partnership between private sector and government. “The President’s cybersecurity policy official should work with relevant departments and agencies and the private sector to examine existing public-private partnership and information sharing mechanisms to identify or build upon the most effective models.” This is one of many recommendations that helped paved the way for new partnerships and documented strategies.

2.5 The Comprehensive National Cybersecurity Initiative (CNCI)

The recommendations from the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. Therefore the CNCI developed twelve initiatives to play a role in supporting the achievement of many of the key recommendations of President Obama’s Cyberspace Policy Review, see table 2.

Table 2 CNCI Initiatives

1	Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.
2	Deploy an Intrusion Detection System across the Federal Enterprise.
3	Pursue deployment of intrusion prevention systems across the Federal Enterprise.
4	Coordinate and redirect research and development (R&D) efforts.
5	Connect cyber ops centers to ensure situational awareness.
6	Develop and implement a government-wide cyber counter-intelligence (CI) plan.
7	Increase the security of our classified network.
8	Expand cyber education.
9	Define and develop enduring “leap-ahead” technology, strategies and programs.
10	Define and develop enduring deterrence strategies and programs.
11	Develop a multi-pronged approach for global supply-chain risk management.
12	Define the Federal role for extending cybersecurity into critical infrastructure domains.

Of particular interest is initiative #5, Connect current cyber ops centers to enhance situational awareness. The initiative states, “there is a pressing need to ensure that government information security offices and strategic operations centers share data regarding malicious activities against federal systems, consistent with privacy protections for personally identifiable and other protected information and as legally appropriate, in order to have a better understanding of the entire threat to government systems and to take maximum advantage of each organization’s unique capabilities to produce the best overall national cyber defense possible. This initiative provides the key means necessary to enable and support shared situational awareness and collaboration across six centers that are responsible for carrying out U.S. cyber activities (Obama CNCI 2009).”

2.6 International Strategy for Cyberspace

In May 2011, President Obama released his International Strategy for Cyberspace although the Administration had previously addressed the policy challenges surrounding cyber technologies the document “is the first time our Nation has laid out an approach that unifies our engagement with international partners on the full range of cyber issues (Obama International Strategy for Cyberspace 2011).”

The strategy seeks to build on prior successes as well as recognize the challenges such as; “the theft of intellectual property threatens national competitiveness and the innovation that drives it (Obama International Strategy for Cyberspace 2011).”

It further discusses one important area regarding the future we seek, a secure and reliable cyberspace that endures. “For cyberspace as we know it to endure, our networked systems must retain our trust. Users need to have confidence that their data

will be secure in transit and storage, as well as reliable in delivery. Vulnerability reduction will require robust technical standards and solutions, effective incident management, trustworthy hardware and software, and secure supply chains. Risk reduction on a global scale will require effective law enforcement; internationally agreed norms of state behavior; measures that build confidence and enhance transparency; active, informed diplomacy; and appropriate deterrence. Finally, incident response will require increased collaboration and technical information sharing with the private sector and international community (Obama International Strategy for Cyberspace, 2011).”

Lastly it defines one of the policy priorities as; improve the security of the of the high-tech supply chain, in consultation with industry. “The operation of critical networks and information infrastructures depends on the assured availability of trustworthy hardware and software. Vulnerabilities in the supply chain can enable attacks on the integrity, availability, or confidentiality of networks and the data they contain. Exploitation of these vulnerabilities impairs economic performance and national security. The United States will work with industry and international partners to develop best practices for protecting the integrity of information systems and critical infrastructure. In this way, we will greatly enhance the security of the globalized supply chains on which free and open trade depend (Obama International Strategy for Cyberspace, 2011).”

2.7 DoD Strategy for Operating in Cyberspace

The DoD released its cyberspace strategy in July 2011. “The DoD working with its interagency and international partners, seeks to mitigate the risks posed to U.S. and allied cyberspace capabilities, while protecting and respecting the principles of privacy and

civil liberties, free expression, and innovation that have made cyberspace an integral part of U.S. prosperity and security. How the Department leverages the opportunities of cyberspace, while managing inherent uncertainties and reducing vulnerabilities, will significantly impact U.S. defensive readiness and national security for years to come (DoD Strategy for Operating in Cyberspace 2011).”

The DoD strategy points out that “foreign cyberspace operations against U.S. public and private sector systems are increasing in number and sophistication. DoD networks are probed millions of times every day, and successful penetrations have led to the loss of thousands of files from U.S. networks and those of U.S. allies and industry partners. Moreover, this threat continues to evolve as evidence grows of adversaries focusing on the development of increasingly sophisticated and potentially dangerous capabilities (DoD Strategy for Operating in Cyberspace 2011).”

“While the threat to intellectual property is often less visible than the threat to critical infrastructure, it may be the most pervasive cyber threat today. Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies. As military strength ultimately depends on economic vitality, sustained intellectual property losses erode both U.S. military effectiveness and national competitiveness in the global economy (DoD Strategy for Operating in Cyberspace 2011).”

Cyber attacks are not a future threat; the Nation faces the threat of cyber attack and constant intrusion efforts today. Recent high profile intrusions highlight the threat to

U.S. businesses and critical infrastructure, and they underscore the need for a strategy for DoD to work closely with the Defense Industrial Base and support DHS in its efforts in other critical infrastructure sectors. Therefore, the DoD strategy made this one of their five strategic initiatives: “DoD will partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.”

2.8 DIB Cyber Security/Information Assurance (CS/IA) Partnership

In January 2010 the DoD issued an instruction which directed the conduct of DIB CS/IA activities to protect unclassified DoD information that transits or resides on unclassified DIB information systems and networks. However, DoD initially started partnering with the DIB to increase the protection of sensitive information in 2007. The new instruction stated “the DoD policy as:

- Establish a comprehensive approach for protecting unclassified DoD information transiting or residing on unclassified DIB information systems and networks by incorporating the use of intelligence, operations, policies, standards, information sharing, expert advice and assistance, incident response, reporting procedures, and cyber intrusion damage assessment solutions to address a cyber advanced persistent threat
- Increase DoD and DIB situational awareness regarding the extent and severity of cyber threats in accordance with National Security Presidential Directive 54/Homeland Security Presidential Directive 23
- Create a timely, coordinated, and effective CS/IA partnership with the DIB, developing operating guidance and undertaking activities that:

- Maintain a DoD-DIB Collaborative Information Sharing Environment (DCISE), to facilitate DoD coordination of threat information sharing and measures enabling the protection of unclassified DoD information transiting or residing on DIB information systems and networks
- Develop procedures for sharing DoD cyber threat information, unclassified and classified, with the DIB
- Share DoD computer network defense and CS/IA best practices with the DIB” (DoD 2010)

Building upon this program, DoD also established a pilot public-private sector partnership intended to demonstrate the feasibility and benefits of voluntarily opting into increased sharing of information about malicious or unauthorized cyber activity and protective cybersecurity measures, an effort called the DIB Cyber Pilot. The program helped a small number of DIB companies protect defense-related information on their computer networks from the most serious intruders was enacted by the DCISE group. Essentially, the DoD and DHS share classified threat information and the know-how to employ it with participating defense companies or their Internet service providers to help them in defending their computer networks from attack or exploitation (Pellerin 2011).

2.9 Joint Cybersecurity Services Pilot (JCSP)

“The Joint Cybersecurity Services Pilot (JCSP) extends the existing operations of the Defense Industrial Base (DIB) Exploratory Cybersecurity Initiative (DIB Opt-In Pilot) and shifts the operational relationship with the commercial service providers (CSPs) in the pilot to DHS. The JCSP is part of overall efforts by DHS and DoD to enable the

provision of cybersecurity capabilities enhanced by U.S. government information to protect critical infrastructure information systems and networks. The purpose of the JCSP is to enhance the cybersecurity of participating DIB critical infrastructure entities and to protect sensitive DoD information and DIB intellectual property that directly supports DoD missions or the development of DoD capabilities from unauthorized access, exfiltration, and exploitation (DHS, 2012)”.

“Although researchers said the DIB pilot had demonstrated the concept of information sharing, they also cited deficiencies in the way it was implemented. The test program, relied on NSA “signatures” or fingerprints of malicious computer code that in initial stages were “stale when deployed” and in many cases did not prevent intrusions that the companies could not have blocked themselves, according to the report, which was not publicly released by the Pentagon but was shared with Congress. The study underscores the operational, legal and policy challenges in building a robust defense of critical U.S. computer networks as foreign rivals and other adversaries seek to penetrate systems, steal data and perhaps lay the groundwork for a destructive attack (Nakashima 2012).” Therefore, time will tell if the JCSP will overcome the challenges and continue to push the successes the U.S. Government has had in the cyber realm.

It is clear that the U.S. Government has made progress in cyberspace over the last few years. Steve Schleien, principal director for cyber in the office of the undersecretary of defense for policy, stated during an interview with American Forces Press Service in October 2001, “Our cyber defense improvement has come from having the strategy in place, having the Cyber Command and the service cyber components taking a serious

look at day-in, day-out coordination of cyber defenses, and the knowledge we have of what our adversaries are doing and how to deal with it” (Pellerin 2011). However, it is also clear that the DoD continues to face challenges in its cyber activities.

In a GAO report issued in July 2011, they made four recommendations that the DoD: “(1) establish a timeframe for deciding on whether to complete a separate joint cyberspace publication and for updating the existing body of joint publications, (2) clarify command and control relationships regarding cyberspace operations and establish a timeframe for issuing the clarified guidance, and (3) more fully assess cyber-specific capability gaps, and (4) develop a plan and funding strategy to address them. DOD agreed with the recommendations.” (US GAO 2011)

As the DoD continues to make strides in its cyber activities, specifically with working hand in hand with the DIB partners it may be appropriate to evaluate whether implementing a cyberspace maturity model could help increase our overall security.

2.10 Capability Maturity Models

“In its simplest form, a maturity model is an organized way to convey a path of experience, wisdom, perfection, or acculturation. The subject of a maturity model can be an object or things, ways of doing something, characteristics of something, practices, or processes. For example, a simple maturity model could define a path of successively improved tools for doing math: using fingers, using an abacus, using an adding machine, using a slide rule, using a computer, or using a hand-held calculator. Thus, a hand-held calculator may be viewed as a more mature tool than a slide rule” (Caralli 2011).

“A capability maturity model such as the Capability Maturity Model (CMM) is a much more complex instrument, with several distinguishing features. One of these features is that the maturity dimension in the model is a characterization of the maturity of *processes*. Thus, what is conveyed in a capability maturity model is the degree to which processes are institutionalized *and* the degree to which the organization demonstrates process maturity” (Caralli 2011).

The CMM is a registered service mark of Carnegie Mellon University (CMU) and is a development model that was created after study of data collected from organizations that contracted with the U.S. Department of Defense, who funded the research. This model became the foundation from which CMU created the Software Engineering Institute (SEI). The Capability Maturity Model (CMM) was originally developed as a tool for objectively assessing the ability of government contractors' processes to perform a contracted software project. The CMM is based on the process maturity framework first described in the 1989 book *Managing the Software Process* by Watts Humphrey. It was later published in a report in 1993 (Technical Report CMU/SEI-93-TR-024 ESC-TR-93-177 February 1993, *Capability Maturity Model for Software*, Version 1.1) and as a book by the same authors in 1995.

Though the CMM comes from the field of software development, it is also used as a general model to aid in improving organizational business processes in diverse areas; for example in software engineering, system engineering, project management, software maintenance, risk management, system acquisition, information technology (IT), services, business processes generally, and human capital management. The CMM has

been used extensively worldwide in government offices, commerce, industry and software-development organizations.

The CMM model proved useful to many, but its application in software development has sometimes been problematic. Applying multiple models that are not integrated within and across an organization could be costly in training, appraisals, and improvement activities. The Capability Maturity Model Integration (CMMI) project was formed to sort out the problem of using multiple models for software development processes, thus the CMMI model has superseded the CMM model, though the CMM model continues to be a general theoretical process capability model used in the public domain.

CMMI is a process improvement approach that provides organizations with the essential elements of effective processes, which will improve their performance. CMMI-based process improvement includes identifying an organization's process strengths and weaknesses and making process changes to turn weaknesses into strengths.

There are three CMMI models. Each model shares practices with the other two models and has practices that are unique. CMMI models are collections of best practices and process improvement goals that organizations use to evaluate and improve their processes. These goals and practices are organized into intuitive groups called "process areas." An organization chooses its path to excellence by focusing on the process areas most important to its business objectives.

The CMMI for Acquisition (CMMI-ACQ) model provides guidance to organizations that manage the supply chain to acquire and integrate products and services to meet the needs of the customer.

The CMMI for Development, (CMMI-DEV) model is used for process improvement in organizations that develop products and services. CMMI-DEV provides guidance to improve the effectiveness, efficiency, and quality of their product and service development work.

The CMMI for Services (CMMI-SVC) model provides guidance to organizations that establish, manage, and deliver services that meet the needs of customers and end users.

After determining which model is most applicable to an organization they strive to achieve a certain maturity level within the model and are subsequently appraised. An appraisal is an activity that helps them to identify strengths and weaknesses of the organization's processes and to examine how closely the processes relate to CMMI best practices. Preparing for an appraisal helps an organization to do any of the following:

- Plan an improvement strategy for your organization
- Determine the CMMI levels that represent how well your organization's processes conform to CMMI
- Mitigate risks for product and service acquisition, development, and monitoring
- Demonstrate to customers and business partners the soundness of your processes by having your appraisal results available on the Published Appraisal Results (PARS) site.

The Standard CMMI Appraisal Method for Process Improvement (SCAMPI) is the official CMMI appraisal method used to evaluate organizations' processes and provide ratings. SEI trains and certifies lead appraisers which are trained teams of professionals in the appraisal of one or more CMMI process areas to determine an organization's process capability and/or maturity level. There are hundreds of organizations that use CMMI have been appraised, a complete current list can be found at <http://sas.sei.cmu.edu/pars/pars.aspx>

2.11 Reference Engineering Framework Defined

The Computer Emergency Response Team- Resilience Management Model (CERT-RMM) is the foundation for a process improvement approach to security, business continuity, and aspects of IT operations management. It establishes an organization's resilience management process: a collection of essential capabilities that the organization performs to ensure that its important assets stay productive in supporting business processes and services. The model provides guidance for measuring the current competency of essential capabilities, setting improvement targets, and establishing plans and actions to close any identified gaps.

Although CERT-REF is a process improvement model, it is not considered a part of the SEI's Capability Maturity Model Integration framework and is not intended to be integrated with existing CMMI models. However, features of CMMI have been used where practical to provide a familiar structure for those who are already users of existing process models and to facilitate transition, adoption, and integration by established communities of practice in process improvement.

“The ultimate goal in CERT-RMM is to ensure that operational resilience processes produce intended results (such as improved ability to manage incidents or an accurate asset inventory), and as the processes are improved, so are the results and the benefits to the organization. Because CERT-RMM is a process-focused model at its core, it was perfectly suited for the application of CMMI’s capability dimension. Thus, the CERT-RMM constitutes a maturity model that has a capability dimension. However, this is not the same as a *capability maturity* model, since CERT-RMM does not yet provide an *organizational* expression of maturity (Caralli 2011).”

The researcher believes the CERT-RMM could be utilized to make a viable Cybersecurity Maturity Model.

2.12 A Proposed Cybersecurity Maturity Model

The researcher proposes utilizing the CERT-RMM model to help the DIB identify any weak areas and where improvements are needed, specifically in improving their cyberspace security. There have been many information security maturity models published over the years, some have included aspects of cyberspace security and others have not. Cyberspace security can be argued to be a subset of overall information security however; it can not be assumed that if you are great in information security, you are great in cyberspace security.

One challenge with cyberspace security is the speed of technology. Some futurists have moved beyond Moore’s law and are predicting a period where progress in technology occurs almost instantly. “Moore’s Law--which states that the number of transistors on a given chip can be doubled every two years--has been the guiding

principle of progress in electronics and computing since Moore first formulated the famous dictum in 1965 (Kanellos 2003).” Therefore, a traditional capability maturity model (CMM) can be viewed as outdated; whereby as soon as an organization obtains a desired maturity level, they rest and potentially let their proverbial guard down while technology is continually introduced. This research explores implementing a different maturity model, the CERT resilience management model (CERT-RMM).

The CERT-RMM is a maturity model that focuses on the operational resilience from a process perspective, which allows for the application of process improvement tools and techniques. This model allows the ability to incrementally improve processes in individual process areas. Each process area can be defined by a capability level, but there are no maturity levels, as this model examines organizations’ operational resilience processes. An organization’s processes, especially in cyberspace, should adjust frequently to new emerging demands, thus their processes should not mature and further, those processes should be measured by how resilient to change each process is.

The researcher chose to include 7 process areas from the CERT-RMM to include in the initial Cybersecurity Maturity Model. By incorporating these areas together and subsequently appraising each process area, an organization is able to determine its capability level within cybersecurity as well as their resiliency to securing sensitive information. The proposed Cybersecurity Maturity Model will be discussed further in chapter III.

III. Research Methodology

I personally think intellectual property is an oxymoron. Physical objects have a completely different natural economy than intellectual goods. It's a tricky thing to try to own something that remains in your possession even after you give it to many others.

John Perry Barlow

3.1 Introduction

Cyberspace has become an ideal medium for stealing intellectual property. Hackers can easily penetrate systems that transfer enormous amounts of data. America's corporations and all levels of government (local, state and federal) have a very hard time identifying specific perpetrators. As pointed out in chapter II, the DIB is just at the cusp of addressing the Cyber threat. It is evident that not all Defense Department contractors have the resources of the larger companies therefore there are varying levels of efforts throughout the DIB to protect their own intellectual property as well as DoD's sensitive information. Responding to a Cyberspace incident is still relatively in its infancy. Combine this fact with limited resources, lack of understanding, and the difficulty of detecting a Cyber incident; it brings to the forefront the need for concrete guidance for which a DIB organization can use to address the cyber threats. Additionally, the DoD needs a means to determine status of respective DIB Cybersecurity.

The goal of this research effort is to develop and refine a model to help the DIB identify both weak areas and where improvements are needed, specifically in improving their cyberspace security. While numerous information security maturity models are in use, few seem to adequately address all aspects of cyberspace security. Cyberspace

security can be argued to be a subset of overall information security but they are not interchangeable. An organization can be “secure” in information security but not “secure” in cyberspace and vice versa.

Due to the pace of technology introduction and implementation, as soon as an organization obtains a desired maturity level, they could be obsolete tomorrow and subsequently are no longer “mature”. An organization must define its processes and put in place resiliency to ensure those processes continue when malicious incidents occur. The model, based on the resilience management model (CERT-RMM), developed and presented by this research is intended to fulfill the need within the DIB. The model can benefit both the DIB and the Department of Defense.

3.2 Overview of Methodology

The methodology for this research was conducted in 3 phases. Phase one involved researching existing Information and Cyber Security Maturity Models; comparing those existing models to assist in developing a Cyberspace Maturity Model and finally create the initial survey. The second phase is where the model is evaluated and validated through the use of a Delphi Study. In phase three, survey results of the Delphi group are analyzed, the final model is presented within this research report, and the recommendations are made concerning the final model and potential areas of research are identified.

3.3 The Delphi Method

The Delphi technique, mainly developed by Dalkey and Helmer (1963) at the Rand Corporation in the 1950s, is a widely used and accepted method for achieving

convergence of opinion concerning real-world knowledge solicited from experts within certain topic areas. The technique is designed as a group communication process which aims to achieve a convergence of opinion on a specific real-world issue. It also documents facts and the opinions of the panelists, while avoiding the pitfalls of face-to-face interaction, such as group conflict and individual dominance (Rowe 1991). “The Delphi technique is well suited as a method for consensus-building by using a series of questionnaires delivered using multiple iterations to collect data from a panel of selected subjects (Hsu 2007)”. Delphi, in contrast to other data gathering and analysis techniques, employs multiple iterations designed to develop a consensus of opinion concerning a specific topic (Ludwig 1994).

This iterative process of rounds and analysis continues until there is a convergence of opinion (consensus) or until a point of diminishing returns is reached (where panelists’ opinions do not vary significantly by round) (Erffmeyer 1986). The feedback process allows and encourages the Delphi participants to reassess their initial judgments about the information provided in previous iterations. Thus, in a Delphi study, the results of previous iterations regarding specific statements and/or items can change or be modified by individual panel members in later iterations based on their ability to review and assess the comments and feedback provided by the other Delphi panelists (Hsu 2007). The comments and feedback will also be useful to this study—the feedback submitted by experts in the field can provide important insights into the strengths and weaknesses of the proposed model.

3.4 Phase I: Cyberspace Security Model Development

In this phase, the scope of the research project is identified and the model is developed, methodology and criteria for evaluating and validating the proposed model are established, and the questionnaire is developed to evaluate the proposed model.

3.4.1 Model Research

An initial literature search was conducted using the research tools *360 Multiple Database Search*, *Library Catalog*, *Journal Search* (all available for use through the D'Azzo Research Library at the Air Force Institute of Technology) and the on-line search engine *Google* (www.google.com). Within the *360 Multiple Database Search*, 18 databases are queried with the provided search terms. The databases include: ABI/INFORM, Academic Search, ACM Digital Library, Aerospace Database, AMS MathSciNet, Business Source Premier, Compendex, Energy Citations, IEEE/IET Electronic Library, Inspec, MasterFile Premier, Military & Government Collection, Science Direct Journals Air University Research Information System, D'Azzo Research Library (print holdings), DTIC Technical Reports, NASA Technical Reports Server, TRIS Online and Web of Science. Searches were conducted using key words or phrases containing the following:

- Information Assurance
- Information Security Maturity Model
- Information Technology Security
- Capability Maturity Model
- Maturity Model

- Cybersecurity Maturity Model
- Cyberspace Maturity Model
- Resilience Management Model

Literature searches were conducted periodically throughout the initial phase to garner any recently published information. The literature review was conducted to determine 1) if a Cybersecurity Maturity Model existed, 2) if so, could it be applied to the DIB in its current format and 3) if a model does not exist, could one be developed and applied to the DIB to address their cybersecurity needs?

3.4.2 Model Development

The literature review revealed: 1) there are numerous traditional information security models in existence and 2) there are a variety of non-specific capability maturity models that could be applied to various functions within an organization; neither of these approaches are easily applied in Cybersecurity due to its ever-changing environment (threat vectors, technology updates, etc.). However, one journal submission entitled “The Community Cyber Security Maturity Model (CCSMM)” (White 2011) presents a maturity model for state and local officials to use in response to cyber incidents. The CCSMM, figure 1, is a 5 tiered model in the traditional sense of a maturity model. The model is a result of funding from the DHS and the DoD; the model has been started in six states. “The model has proven to be useful in the communities that have embarked on a path to develop a viable and sustainable security program, but the model is still too new for any state or community to have advanced beyond the lower levels of the model.”

(White 2011) The model is intended to provide a yardstick which can be used to determine how mature a community's cyber security program is.

The researcher felt the CCSMM could possibly be utilized within the DIB but, the model would require significant modification. The CCSMM was worthy of consideration for the following reasons: 1) the model contains five maturity levels, ranging from minimal cyber preparedness (initial) to a demonstrated cyber awareness, integration and ability to assess fusion capability (vanguard) and 2) in order to transition from one level to the next, metrics need to be developed. These metrics include, the current security posture, information sharing mechanisms, training required by various personnel and identify the mechanisms that will be used to test or evaluate the preparedness of the community. The CCSMM is community based and is aimed at local and state officials who are developing a cyber security program in the vein of cyber response.

Due to the continual loss of sensitive data by known common methods the researcher believes a Cybersecurity model for the DIB needs to be more preventative rather than responsive and a model should stress continuous improvement. In a 2012 data breach investigation study, conducted by the Verizon RISK team, they found that "most victims fell prey because they were found to possess an (often easily) exploitable weakness rather than because they were pre-identified for attack. Whether targeted or not, the great majority of victims succumbed to attacks that cannot be described as highly difficult. It's not surprising that most breaches were avoidable (at least in hindsight) without difficult or expensive countermeasures. And finally, victims usually don't know about their

breach until a third party notifies them, and almost all breaches are avoidable without difficult or expensive corrective action” (Verizon 2012).

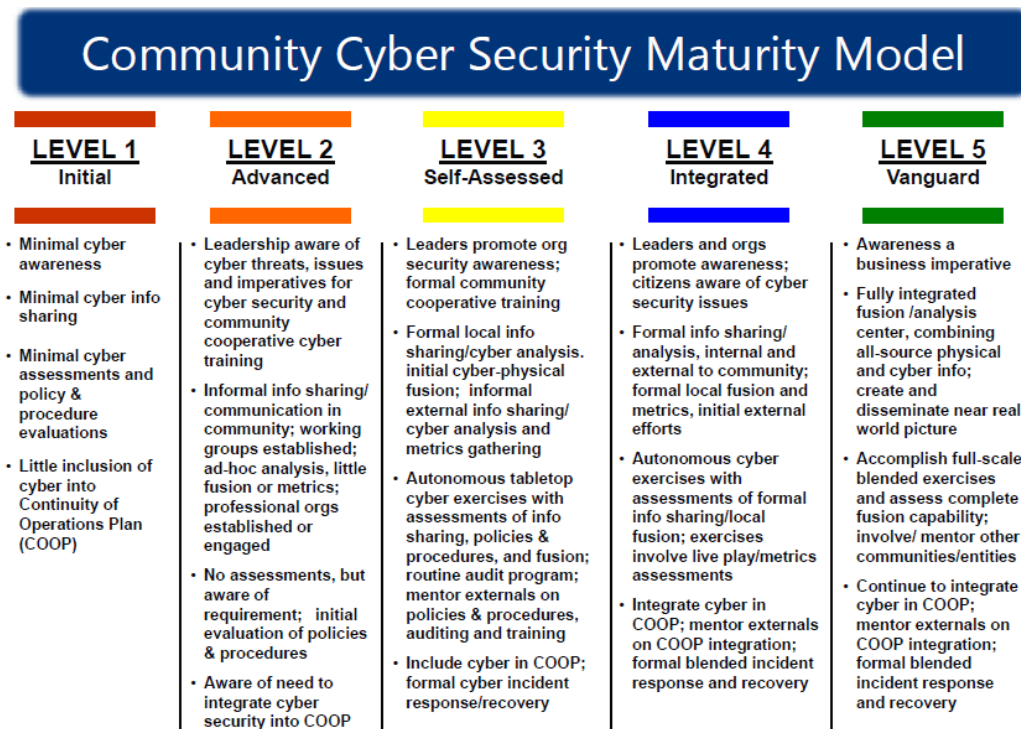


Figure 1 Community Cyber Security Maturity Model

As further evidence that an adequate cyberspace maturity model does not yet exist, “The White House launched a new initiative designed to help companies in the electric power industry measure the maturity of their security programs against a new maturity model. The Electric Sector CyberSecurity Risk Maturity Model Pilot started in January 2012 is meant to help the utility companies find their weak spots and where they need to improve. It is not exactly clear what the maturity model will consist of.” (Fisher 2012) Although, the Electric Sector maturity model was not available in time for this

research paper, the call for action by the White House and the fact that one has been developed for local communities does validate that one or more Cyber Security Maturity Models are needed to specifically address the deficiencies within securing the DIB cyberspace.

One model that was discovered during the literature review was the Computer Emergency Response Team-Resilience Management Model (CERT-RMM) developed by the Software Engineering Institute at Carnegie Mellon. The CERT-RMM is a capability model for operational resilience management. It has two primary objectives: 1) establish the convergence of operational risk and resilience management activities such as security, business continuity, and aspects of IT operations management into a single model and 2) apply a process improvement approach to operational resilience management through the definition and application of a capability level scale that expresses increasing levels of process improvement. The CERT-RMM contains 26 process areas grouped into 4 categories (Engineering, Enterprise Management, Operations Management, and Process Management). The CERT-RMM peaked the researcher's interest for the following reasons: the model is tailorable and the model measures operation resilience and processes. The CERT-RMM is tailorable because, the model scope is determined by selecting the desired process areas from the 26 specific CERT-RMM process areas. The process areas are chosen based on the objectives and business case for the improvement effort in an organization, in this case Cybersecurity. The CERT-RMM differs from a traditional capability maturity model (CMM). "In a traditional CMM, the *capability* dimension describes the degree to which a process has been institutionalized. The

maturity dimension is achieved by raising the *capability* of a *set of process* areas in a manner prescribed by the model” (Caralli 2011). On the other hand, the CERT-RMM contains a capability dimension but does not contain a maturity dimension. The CERT-RMM “describes operational resilience management from a process perspective, the application of process improvement tools and techniques as well as provides for better and more sophisticated measurement methodologies. The ultimate goal for the CERT-RMM is to ensure operational resilience processes produce intended results and as the processes improve the organization benefits. The CERT-RMM is a capability model—grounded in process-and providing a path for improving capability. Therefore, with the CERT-RMM in its current form an organization can not “rest on its laurels” a state that it is mature, rather its processes are capable and resilient to future misfortunes.

The researcher determined that a Cybersecurity model could be constructed utilizing the established CERT-RMM. After extensively reviewing each of the 26 process areas within the CERT-RMM, process areas were selectively chosen that explicitly mentioned information or computer security. A total of 7 process areas were identified, based on the process area purpose and description as described in the book, CERT Resilience Management Model, A Maturity Model for Managing Operational Resilience (Caralli 2011). Utilizing these 7 process areas, along with their 78 sub-process areas, an initial Cybersecurity Maturity Model was developed while keeping in mind the key points identified during the literature review and the overall research goal of how to secure the sensitive information within the DIB. The initial Cybersecurity Maturity Model can be found at appendix B.

3.4.3 Questionnaire Development

The Cybersecurity model, developed from 7 process areas of the CERT-RMM, was presented to the Delphi panel and was evaluated for comprehensiveness, accuracy, completeness, and usefulness. A questionnaire was created to ask open-ended questions in order to garner each panel member's thoughts and opinions regarding the proposed Cybersecurity model. The following question was presented to assess the comprehensiveness of the model:

- I've introduced the CERT-Resilience Management Model as a way to access Cyberspace security, was it clear with its intent?
- What are its strengths?
- What are its weaknesses?

The following question was presented to assess the accuracy of the model:

- Describe how successful the proposed Cyberspace Maturity Model captures the vital processes that should be evaluated in determining an organizations Cyberspace security.

The following question was presented to assess the usefulness of the model:

- Please explain, why or why not, implementing a Cyberspace Maturity Model could help the DIB better focus their efforts in defending their Cyberspace.
- Are you in favor of having this Cyberspace Maturity Model in place to appraise DIB members in measuring their Cyberspace security? Please list you supporting reasons.
- What recommendation would you make to make this model more useful?

The following question was presented to assess the completeness of the model:

- List and describe any processes you would include or delete from the proposed Cyberspace Maturity Model.

The above open ended questions allowed the panel members to not only evaluate the proposed model but also make recommendations; thus contributing significantly to the overall model development.

3.4.4 The Study Population

The population of interest in this study was the entire Defense Industrial Base (not just the DIB contractors). It seems as though Cybersecurity has become the en vogue term within the past 5 years but as this research has demonstrated, it is for good reason that each level of government and private sector is starting to take heed. By successfully developing and implementing a Cyberspace Maturity Model within the DIB population it may aide the other sectors within the United States that also need immediate attention to help secure their critical information.

The need and aspirations are at hand as evident by the recent White House announcement which launched the Electric Sector Cybersecurity Risk Maturity Model Pilot initiative, in January 2012, to help companies in the electric power industry measure the maturity of their security programs against a new maturity model (Fisher 2012). Additionally, this study could provide insight to other critical infrastructure areas such as the financial networks.

3.4.5 The Delphi Panel Participants

The first task within the Delphi Method is to create the panel. “Three kinds of panelists are ingredients for creating a successful mix: stakeholders, those who are or will be directly affected; experts, those who have an applicable specialty or relevant experience; and facilitators, those who have skills in clarifying, organizing, synthesizing, stimulating... plus, when it seems appropriate, individuals who can supply alternative global views of the culture and society” (Linstone 1975) .

There is no definitive authoritative number that a Delphi panel must contain. However, one guideline is that if the Delphi participants all come from the same discipline (e.g., computer programmers) the general rule of thumb is 15-30 participants, whereas a more heterogeneous population (expertise in the same area, but pulled from different social/professional levels) would only require 5-10 participants (Clayton 1997).

The 10 members of the Delphi panel for this research effort comprise a heterogeneous group of experts and the total number of participants should allow for an adequate diversity of inputs. For purposes of the technique, the individuals in the group did not know who was participating nor who made which comments – anonymity has been shown to increase creativity and idea generations (Linstone 1975).

Table 1 profiles the division of expertise the Delphi members are currently working in, Table 2 lists the breakdown of participants by organizational area and Table 3 lists the breakdown by functional area.

Table 3 Area of Expertise

<u>Area of Expertise</u>	<u>Delphi Participants</u>
Computer Network Attack	2
Computer Network Exploitation	3
Computer Network Defense	5

Table 4 Breakdown by Organizational Area

<u>Organizational Area</u>	<u>Delphi Participants</u>
Department of Defense (DoD)	6
Private Sector	4

Table 5 Breakdown by Functional Area

<u>Functional Area</u>	<u>Delphi Participants</u>
Defense Industrial Base (DIB) - Contractors	3
Unit Commander Perspective – (1 current and 1 former) Acquisition and Network Warfare	2
Combatant Command	1
Acquisition	1
Academic	1
Security Threat Consultant	1
Cyber Crime Specialist	1

3.5 Phase II: Model Evaluation and Validation

In this phase, the questionnaire developed in phase I is presented to the Delphi panel for their use in evaluating the model developed in phase I. A study primer was sent to each participant explaining: Delphi Studies, the research issue, the research purpose, maturity models, capability maturity models, the CERT-RMM model and the proposed Cybersecurity Maturity Model.

3.5.1 Round One

Prior to round one, the questionnaire was pilot tested with one classmate within the AFIT Cyber Warfare program. The questionnaire was reviewed and a few minor clarifying changes were made based on feedback from the pilot study.

To begin Round one, a Delphi Panel primer (Attachment A), the proposed Cybersecurity Maturity Model (Attachment B), and the questionnaire (Attachment C) was sent out to each participant via e-mail. The primer and questionnaire consisted of textual information, as an MS Word 2007 document and the proposed Cyberspace Maturity Model) consisted of a MS Excel 2007 spreadsheet. Participants were asked to first read the primer, second refer to the proposed Cybersecurity Maturity Model and third complete the questionnaire. The questionnaire consisted of 11 open-ended questions. The participants were asked to record and save their responses electronically, and then send the completed questionnaire back to me via e-mail. Ten questionnaires were sent out and nine were received back for a 90% completion rate. The initial round took just over three weeks (24 days), after which the results were collated and organized

for further group consideration in the second round. The analysis of round one results is described in Chapter IV.

3.5.2 Round Two

In the second round, the questionnaire was modified to include the individual participant responses from round one. The questions for round two remained relatively unchanged from round one, although some questions included additional clarifying information. The questions were now worded as: do you agree with, please rank the following, and/or please mark agree or disagree with the following. By asking the same questions from round one, plus providing additional information and grouping the participant's responses within each question, the panel had the opportunity to view and evaluate each participant's responses and potentially reach a consensus.

The responses from the open-ended questions in the round one questionnaire that recommended changes to the proposed Cybersecurity model were analyzed and the recommendation were incorporated into a modified Cybersecurity model for evaluation in round two.

The round two instructions (Attachment D), the modified Cybersecurity Maturity Model (Attachment E), and the round two questionnaire (Attachment F) was sent out to each participant via e-mail. The questionnaire consisted of 9 questions, as a result of two questions being combined (question 7 and 8) and one question (question 11) being eliminated, as it was not applicable for round two. Ten questionnaires were sent out and nine were received back for a 90% completion rate. Round two took a little more than

two weeks (18 days), after which the results were collated and organized for further analysis by the researcher. The analysis of round two results is described in Chapter IV.

3.6 Phase III: Analysis of Delphi Study Results, Model Modification and Recommendations for Future Research

In phase three, the survey results of the Delphi group are analyzed and any modification suggested by individual committee members are either incorporated into the final framework or are identified for further research. Recommendations are made based on the analysis of the questionnaire results and the model is revised to reflect the conclusion of the analysis performed in Chapter IV. Future research topics are identified in Chapter V.

IV. Results and Analysis

4.1 Overview

Analysis from two rounds of the Delphi panel have been summarized and presented in the summary of results. The summary describes a review of how the Delphi was executed and also discusses the questions relating to cybersecurity within the DIB from the questionnaires. The section on evaluating the model explains those questions pertaining to a proposed Cybersecurity Maturity Model. Finally, the research results section reiterates the research questions and provides the panels assessments, concerns and recommendations.

4.2 Summary of Results

The Delphi committee initially consisted of 10 members; however one member was unable to respond during round one. As a response was not received from the same member during round two, the researcher considered the panelist dropped which subsequently left the committee with a total of 9 members. The round one questionnaire consisted of 11 open-ended questions relating to overall cybersecurity within the participants organization and questions relating to valuating the proposed Cybersecurity model for use within the DIB. Of the 9 members, all (100%) responded to questionnaire in round one. The panelists' comments were analyzed and incorporated into the round two questionnaire.

The second round of the Delphi process consisted of 9 questions, as a result of two questions being combined (question 7 and 8) and one question (question 11) being

eliminated, as it was not applicable for round two. Of the 9 members, all (100%) responded to questions in round one.

The Delphi panel responses were analyzed to determine: 1) if a consensus was reached, 2) if panelists' opinions did not vary from round to round and 3) potential areas for further research. For this study, the questionnaire was broken-down into 3 sections although not explicit to the panel. Section one contained 4 questions regarding overall cybersecurity relating to the DIB, section two contained 1 question pertaining to a generalized maturity model for cyberspace and section three contained 5 questions to analyze the proposed Cybersecurity Maturity Model as well as determine its applicability in aiding the DIB in securing their sensitive information.

A Consensus (total agreement) was reached on 6 of the 8 measureable questions, recall that one question (question 1) was not intended to be measureable. The panel opinions did not vary between round one and round two, therefore opinion stability was reached on the remaining 2 of 8 questions. The analysis follows:

Question 1: The first question presented to the panel was to describe your experience with Cybersecurity and Information Security, this question was asked to gain the experience level within the panel. In addition to the panel representation depicted in tables 1, 2 and 3, the following panel statistics were reported:

- Each panel participant has a minimum of 10 years experience in Information Security and/or Cyber
- 3 panel members hold PhD's in a Cyber discipline
- All 10 panel members are currently working in the Cyber realm and are therefore maintain currency in this highly volatile environment

Consensus

Question 2: What do you think the top problems your organization faces in providing Cybersecurity?

- Round One- Respondents reported from their individual organizations perspective. The researcher aggregated the results and provided the reported problems back to the group in round two. The problems reported were:
 - 4 members specifically mentioned training of personnel or lack of real cyber expertise
 - 4 members specifically mentioned Management/Management support/Bureaucracy of Corporation/How Organized
 - 3 members specifically identified: limited resources/current budget level/budgetary priority
 - Other identified problem areas:
 - Involving security from project birth
 - Getting programmers to understand security, vulnerabilities, and exploitations
 - Penetration testing with techniques of hackers
 - Sharing of incident information; openly
 - Testing stability and security of unique software development efforts
 - Finding security incidents even while monitoring
 - Maintaining fully patches systems; patches constantly coming out
- Round Two- Respondents were asked if they were largely in agreement with the problems identified above?

All respondents reported, yes they are in agreement with the identified problems, thus the group reached consensus on question two.

Question 4: There are frequent reports of cyber intrusions (penetrations into a network) which has resulted in the loss of sensitive information and intellectual property. When this happens to the DoD and/or a DIB member, what effects could it have on your organization?

- Round One- Respondents reported from their individual organizations perspective. The researcher analyzed the results and provided the reported responses back to the group in round two. The effects reported were:

- Significant financial and liability impact
 - Large impact on national security via the long term “bleeding”
 - Decision makers have near zero visibility into after effects/ongoing risks that intrusions present to mission capabilities
 - When media reports intrusions, attackers change tactics which makes future detection more difficult
 - Compromising U.S. weapon system during development
 - Grave effects-DIB partners may contain system vulnerabilities that could aide the enemy
 - Affects people through loss of PII (personal identifiable information)
 - Affects DoD’s image to U.S. citizens
- Round Two- Respondents were asked to “Please rank the **top 3** effects the loss of sensitive information and intellectual property could have taking the entire DIB (both DoD and DIB contractors) into context.”

The researcher calculated the overall respondent’s rankings. This was done by listing the individuals ranking by each affect, then adding the respective individual rankings, per effect. The 3 affects with the lowest overall score was determined to be the top 3 effects as listed below.

- 1) Compromising U.S. weapon system during development
- 2) Large impact on national security via the long term “bleeding”
- 3) Grave effects-DIB partners may contain system vulnerabilities that could aid the enemy

Question 5: Please explain, why or why not, implementing a Cybersecurity maturity model could help the DIB better focus their efforts in defending their Cyberspace.

- Round One- All respondents reported positively and listed the below reasons of why implementing a Cybersecurity maturity model could help:
 - Provides a framework for prioritizing actions, improvements, comparison benchmarks and goals
 - Provides a common framework for communication exchange and requirements
 - Educate management on the importance of securing the network

- Provides a way for government contract managers to choose the more secure companies (on paper)
 - Improve the security posture and help understand the network “hygiene” of organizations which work together
 - Could give them a plan to improve their security posture
 - Identifies similar goals organizations could work towards
- Round Two- The panel was asked “Given that the panel stated implementing a Cybersecurity maturity model could help the DIB focus their efforts, are you in favor of describing why it would help as:”

A Cybersecurity maturity model could help the DIB better focus their efforts in defending their Cyberspace by providing:

- A common starting point
- A framework for prioritizing actions
- A way to define what improvement means to an organization
- And it can be used as a benchmark for comparison

All respondents replied that yes, the above statement describes why a Cybersecurity maturity model would help the DIB better focus their efforts in Cyberspace.

4.3 Evaluating the Model

This section is dedicated to those questions asked specifically around the proposed Cybersecurity maturity model and the DIB’s potential utilization. One question reached a consensus while four questions did not reach consensus but opinion stability was reached, as the respondent’s views did not change from the previous round.

Consensus

Question 7: Describe how successful the proposed Cybersecurity Maturity Model captures the vital processes that should be evaluated in determining an organizations Cyberspace security.

Question 8: List and describe any processes you would include or delete from the proposed Cyberspace Maturity Model?

These questions were asked separately during round one however, some respondents blended their answers during round one. During round two, question 7 was incorporated into question 8. Therefore, a combined analysis is provided below:

- Round One - The respondents generally responded favorably that the proposed Cybersecurity Maturity Model (appendix B) captured the vital processes and further did not identify any areas that should be deleted. However, the panel offered the following additions:

- The panel suggested including the following additions, however these are currently embedded in the identified processes:

Forensics → Incident Management And Control (IMC)

Audits → Incident Management And Control (IMC)

Tools and Technology → Technology Management (TM)

- The panel suggested including the following additions, these processes were added and are highlighted in the model:

Penetration Testing → Resilient Technical Solution Engineering (RTSE)

Human Factors (abilities of people-skill sets, training, job knowledge, experience, etc) → Organizational Training And Awareness (OTA)

Expand the monitoring section → Added detecting of signatures

Expand incident management & control → Added forensics and share incident information

Round Two- The panel was asked to “Please refer to the updated Cyberspace Maturity Model and review the highlighted areas. Do you feel the proposed Cyberspace Maturity Model captures the vital processes that should be evaluated in determining an organizations Cyberspace security?”

The researcher incorporated the panel’s recommendations into the proposed model and included it for the round two evaluation (appendix E). All respondents replied yes,

the updated proposed model captures the vital processes that should be evaluated in determining an organizations Cyberspace security.

Consensus through Majority

The following questions were asked in an open-ended format during round one, then the researcher presented the results from round one in a matrix and asked the panel to agree or disagree with the respondent's round one answers. The panel results below are presented by majority, more than half the panel identified concurrence with the statement. Therefore, the results are presented after analysis from round one and two.

Question 6: I've introduced the CERT-Resilience Management Model as a way to access Cyberspace security...

- What are its strengths?
 - Operational Resilience
 - Incremental Process Improvement
 - Intended Results
 - Common Framework for Evaluating Processes
 - Coverage of General Principles for Establishing Security Processes
 - Common Framework to help improve Security Capability
 - Model builds on Established Models that may be familiar to Org's
 - Seven Processes and Associated SP's thoroughly cover main ideas in the Cyber Security Space
- What are its weaknesses?
 - Lack of details
 - Hard to Address Deployment Effectiveness in a Real Environment
 - Does not address Abilities of People (skill, training, experience)
 - Model too focused, include: Education, Training and Technology

Question 9: What recommendation would you make to make this model more useful?

- The panel identified numerous recommendations that could make the introduced model more useful during round one. During round two the panel

was asked “please review them and mark your concurrence in the appropriate column.”

- Identify more specific controls for auditing capabilities
- Combine asset management and technology management
- Introduce Associated Scoring- would allow other org’s to understand where accessed org’s- scoring as is limited to ‘does’ or ‘does not’
- Reorganize sections to follow a standard or development lifecycle
- Include context relating to cost with implementation and maintenance of maturity level (Beneficial to both large and small org’s)

The above strengths, weaknesses and recommendations were taken into consideration along with the responses to questions 7 and 8, when updating the proposed Cybersecurity Maturity Model for the panels’ evaluation in round two. Those not incorporated will be reviewed for potential future research in chapter V.

Opinion Stability

The last two questions specifically address securing the DIB’s Cyberspace and whether the proposed Cybersecurity Maturity Model is useful in achieving that goal. Responses to both questions barely deviated, if at all, between rounds, therefore the opinions of the panel reached a stability point.

Question 3: Do you see any problems with requiring all (smaller-larger) members of the DIB to secure their respective Cyberspace (networks computer systems and infrastructure) under their control?

- Round One- The respondents reported:
 - 4 members responded no.
 - 5 members responded yes. Of the yes’s:
 - 3 expressed concerns over resources of smaller companies
 - 1 stated enforcement could be an issue
 - 1 stated there is no way to be 100% secure, especially against a motivated attacker

- Round Two- The researcher provided additional information (below) for round two, then re-asked the same question:
 - If a Cyberspace maturity model was approved and implemented; future request for proposals (RFP) could include a provision such as: demonstration of having achieved a capability level 2 within the Cyberspace maturity model is required or even highly desired. (Much like was used with software acquisition). This could incentivize all DIB members; although this would drive contract prices up it may be worthwhile.
 - Since the Cyberspace maturity model is based on the CERT-RMM there is an established formalized appraisal process with appraisers already trained and in place. The presented Cyberspace maturity model is a more focused model but the appraisers and appraisal process are unchanged.

The results did not change from round one; although the clarifying remarks helped the panel better understand the intent of the Cybersecurity model. The panel reported: 4 members responded no (in favor of requiring all DIB members to secure their Cyberspace), 5 members responded yes (not in favor of requiring all DIB members to secure their Cyberspace). The panel feels that securing Cyberspace is important however most felt that requiring each DIB member to secure their respective Cyberspace under their control could hurt the smaller DIB members. For instance, smaller companies may not have the resources to obtain a prescribed level which may preclude competition. Lastly, some felt the requirement is not measurable, achievable or enforceable.

Question 10: Are in favor of having this Cybersecurity Maturity Model in place to appraise DIB members in measuring their Cyberspace security?

- Round One- The respondents reported:
 - 6 members responded yes.
 - 3 members responded no. The concerns/reservations raised were:

- Model could become compliance based as opposed to addressing real issues surrounding cyber security
 - This CMM could end up being a audit or checkbox used to win contracts
 - Scoring does not provide enough granularity
- Round Two- The researcher provided additional information (below) for round two, then re-asked the same question:
 - The proposed Cyberspace Maturity Model is based on the CERT-RMM which focuses on the processes of an organization and ultimately their operational resilience in those processes. It is a shift from the a Capability Maturity Model (CMM) as in the Cyberspace Maturity Model organizations are assessed by reaching a capability level and within each level how they are improving; thus no maturity is ever achieved.
 - Scoring detail was purposely omitted to focus on which processes to include within the model. However, to reach a particular capability level, an organization must satisfy all of the appropriate goals (Specific Goals and Specific Processes) of the process areas. An organization would receive the lowest level rating of which they satisfied all goals. There is currently no staged representation scoring in the CERT-RMM, but it can be viewed as those organizations that reach a higher capability levels in each process area are exhibiting a higher degree of (maturity).

The clarifying remarks helped the panel better understand their concerns and reservations from round one. The panel reported: 7 members responded yes (in favor of having the proposed Cybersecurity Maturity Model in place to appraise the DIB), 2 members responded no (not in favor of having the proposed Cybersecurity Maturity Model in place to appraise the DIB). Overall, the panel believes the proposed model would be beneficial.

4.4 Research Results

The Delphi panel was asked to answer questions: to help frame the problem of securing sensitive information (question 2, 3 and 4), to facilitate explaining why or why not a Cybersecurity Maturity model could help the DIB (question 5), and to help analyze develop and determine if the proposed Cybersecurity Maturity Model be used to appraise the DIB's Cyberspace security (question 6, 7, 8, 9 and 10).

The panel identified the top 3 affects the loss of sensitive information and intellectual property could have on the entire DIB as:

- 1) Compromising U.S. weapon system during development
- 2) Large impact on national security via the long term "bleeding"
- 3) Grave effects-DIB partners may contain system vulnerabilities that could aid the enemy

In order to address these and other affects of losing sensitive information, the researcher suggested utilizing a maturity model and solicited feedback from the Delphi panel. The panel unanimously agreed that a Cybersecurity maturity model could help the DIB better focus their efforts in defending their Cyberspace. Further, the panel came to a consensus on the proposed Cybersecurity Maturity Model (appendix E). The panel felt that the model captured all the vital processes that should be evaluated in determining an organizations Cyberspace security.

Therefore, the core research question of "Can a Cybersecurity Maturity Model be utilized to assess the level of security the DIB provides to sensitive unclassified DoD information?" is answered by the panel as yes. However, it is in the implementation of a Cybersecurity model that the views of the panel differ. The panel focused on two areas

of implementation: 1) Requiring all members of the DIB to secure their respective Cyberspace under their control and 2) Having the proposed Cybersecurity Maturity Model in place to appraise DIB members in measuring their Cyberspace security.

Requiring all members of the DIB to secure their Cyberspace

The majority (5 out of 9) panelists expressed concerns over the word requiring. The panelists felt that by requiring a certain level it may preclude many smaller companies from competing for government contracts. The smaller companies with less cash reserves and resources might have problems getting approved at a certain level. In the short term this may force smaller companies out of the DIB. One panelist points out that requiring the DIB to secure their cyberspace is not measureable, achievable or enforceable. Lastly, one panelist points out that it is not possible to be 100% secure, especially if an attacker is motivated. If this becomes a requirement it will increase the cost of contract prices.

The researcher feels one panelist summed it up best; “the proposed CMM method demonstrating cyber security capabilities is the correct way to go.” It should not mandate that anyone needs to meet a certain criteria. Instead, it sets forth requirements for each level and then it is up to each organization to decide which level they would like to achieve.” As a result, the researcher concurs with the panel and recommends that the proposed Cybersecurity Maturity Model be a guiding principle versus a mandate that is required. However, as it is a maturity model it does provide 1) a common starting point, 2) a framework for prioritizing actions, 3) a way to define what improvement means to an organization and 4) it can be used as a benchmark for comparison between DIB

members. Consequently, it will incentivize those DIB members who have not taken all measures available and necessary to secure their sensitive information.

Proposed Cybersecurity Maturity Model appraise DIB members

Although the majority (6 out of 9) panelists were in favor of having the proposed Cyberspace Maturity Model in place to appraise DIB members in measuring their Cyberspace security there were some concerns raised. Three panelists identified that the model may just become compliance based rather than addressing the heart of cyber security. One panelist went further by describing; “companies will just buy a widget or hire a subcontractor in order to meet this type of requirement and win contracts. This puts the smaller companies at a disadvantage since they may not have the money to buy the widget/people in order to meet the CMM requirements.” The researcher acknowledges the concern which will be addressed in chapter V, areas for future research.

V. Discussion & Recommendations

“Intellectual property has the shelf life of a banana.” Bill Gates

5.1 Conclusion

For sometime, it has been quite clear that our adversaries have been attacking America’s networks to include the Department of Defense’s, to obtain any and all sensitive information they could obtain. There has been ample evidence, not just proof of the information leaving our networks but most importantly; some of our adversaries have used that sensitive information to mimic America’s cutting edge technology. For example, China’s J-20 looks remarkably similar to the U.S.’s F-22. There are many other examples to include ships, attempted patent filings etc. The entire DIB is now a target, as the adversary looks for the path of least resistance, i.e. least patched/secure network. The purpose of this research was to help the entire DIB secure their sensitive information, possibly with a Cybersecurity Maturity Model.

This research supported, via a Delphi panel, that a Cybersecurity Maturity Model can be developed successfully to better focus the DIB’s efforts and demonstrate an organizations cyber security capability. Further, the model would: 1) establish a common starting point across the DIB, 2) allow an organization to prioritizing their actions in securing their cyberspace, 3) defines what improvement means to an organization and 4) could be used as a benchmark for comparison.

5.2 Recommendations for Future Research

While a Cybersecurity Maturity Model was developed, there are areas that require additional research. One area is how best to implement a Cybersecurity Maturity Model. Even though the Delphi panel liked the proposed model they did not agree with requiring it to be used by all DIB members. More research is needed into how to implement such a model without it eventually becoming compliance based, i.e. a checkbox to win contracts versus a continuum of improving cybersecurity.

Another area where future research is needed pertaining to how best to score the capability levels of organizations; although the proposed model was based on the CERT-Resilience Management Model (RMM), the researcher did not focus on scoring, appraisal method and frequencies. The CERT-RMM is in use by hundred's of organizations but more research is needed to determine if the scoring and appraisal methods would be applicable to a Cybersecurity Maturity Model.

As these areas of future study are researched, the proposed Cybersecurity Maturity Model should then be tested in a trial with DIB members of various sizes; large, medium and small. This trial could yield additional results that may ease those concerns and reservations of this Delphi panel.

5.3 Closing Thought

Cybersecurity has become very important both to National Security and security of organizations at all levels. In fact, at the time of this research, the U.S. Congress is discussing and debating how best to share information between the government and technology companies, in the interest of warding off cyberthreats. The bill entitled

Cyber Intelligence Sharing and Protection Act, or CISPA passed the House of Representatives on 26 April 2012. The U.S. House of Representatives Intelligence Committee's website displays a backgrounder on the bill which stated "Today, the United States government protects itself against cyber espionage by using both classified and unclassified cyber threat information. However, the vast majority of the private sector doesn't get the benefit of the classified threat intelligence that the government already has in its possession. If the government were able to share its classified threat information, the private sector would be able to better defend itself against nation-state actors in cyberspace. An important experiment recently conducted by the Defense Department proves that this can work. The Defense Industrial Base Pilot program provided classified cyber threat intelligence to communications service providers who used it protect defense contractors. The pilot showed that sharing intelligence can enhance private cybersecurity without any government monitoring."

The debate of how to best deal with cyber security may continue at all organizations levels but there is no longer a debate over why cyber security is needed. The researcher believes this report is another small step forward in securing cyberspace.

Appendix A - Delphi Group Primer

What does being a part of a Delphi Study mean?

You are part of a group of experts that provide their opinions and insight on a research topic. The ideas generated are then analyzed and condensed to determine a level of consensus. The Delphi Technique is performed in a series of rounds. This iterative process of rounds and analysis continues until a consensus or stabilization point has been reached. For purposes of the technique, the individuals in the group may know who is participating but will not know who made which comments – anonymity has been shown to increase creativity and idea generation.

What is the Research Issue?

It is well documented that the U.S. Government, its Departments and Agencies as well as private industry has come under Cyber attack in the past several years. In the October 2011, *Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, it is was reported “that the U.S. intelligence community has improved its collaboration to better address cyber espionage in the military and national-security areas” however it went on to say “Corporate America must do its part, too. If we are to ever understand the extent of cyber espionage, companies must be more open and aggressive about identifying, acknowledging and reporting incidents of cyber theft.” Essentially, as the federal agencies have hardened their networks, our adversaries look for alternate paths with vulnerabilities; which greatly increases the odds of success. Our adversaries are aggressively attacking the Defense Industrial Base (DIB) to gain sensitive information.

The Verizon Risk Team said, “The general rule of thumb remains: Some organizations will be a target regardless of what they do, but most become a target because of what they do (or don’t do)”, in the *2011 Data Breach Investigations Report*.

Therefore the core research issue is: How secure is the DIB?

What is the Research Purpose?

In an effort to further the DIB’s cybersecurity, it may be appropriate to implement a capability model or similar framework for Cyberspace Security based on a number of variables. This could allow future contracts between the DoD and a DIB contractor to prescribe a desired level within the framework to ensure a desired level of protection for sensitive information is implemented and maintained.

What is a Maturity Model?

A maturity model is a set of structured levels that describe how well the behaviors, practices and processes of an organization can reliably and sustainably produce required outcomes. A maturity model can provide:

- A common starting point
- A framework for prioritizing actions

- A way to define what improvement means to an organization
- And it can be used as a benchmark for comparison

What is a Capability Maturity Model (CMM) [registered service mark of Carnegie Mellon University]?

A CMM is a more complex instrument than a base maturity model, with several distinguishing features.

- *Maturity Levels*: a 5-level process maturity continuum, from level 1 Initial to level 5 Optimizing
- *Key Process Areas (KPA)*: identifies a cluster of related activities that achieve a set of goals considered important
- *Goals*: the goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way
- *Common Features*: include practices that implement and institutionalize a key process area
- *Key Practices*: describe the elements of infrastructure and practice that contribute to the implementation and institutionalization of the KPAs

What is the CERT-Resilience Management Model (RMM) and how does it differ from a CMM?

The CERT-RMM was developed by Carnegie Mellon University and is a capability model that:

- Focuses on the operational resilience from a process perspective
- Allows the ability to incrementally improve processes in individual process areas
- Each process area can be defined by a capability level (like in a CMM) but differs from a CMM because there are no maturity levels
- The ultimate goal in a CERT-RMM is to ensure that operational resilience processes produce intended results and as processes are improved, so are the results and the benefits to the organization.
- Although CERT-RMM does not currently contain any maturity levels CMU is conducting additional research to see if this is needed in the CERT-RMM.

What Framework is this Research Purposing?

This model is meant to help the DIB identify weak areas and where improvements are needed specifically in improving their cyberspace security. There have been many information security maturity models published over the years, some have included aspects of cyberspace security and others have not. Cyberspace security can be argued to be a subset of overall information security but they are not interchangeable. An organization can be “secure” in information security but not “secure” in cyberspace and vice versa.

The challenge with cyberspace security is the speed of technology. Some futurists have moved beyond Moore’s law and are predicting a period where progress in technology occurs almost instantly; so the implementation of a traditional capability maturity model (CMM) may be outdated. Due to the pace of technology introduction and implementation, as soon as an

organization obtains a desired maturity level, they could be obsolete tomorrow and subsequently are no longer “mature”. An organization must define its processes and put in place resiliency to ensure those processes continue when malicious incidents occur. Therefore, I am proposing implementing the resilience management model (CERT-RMM).

Please refer to the attached capability model when responding to the questions:

The Cyberspace RMM for the DIB can be found at the attached Excel spreadsheet:

* Roll mouse over each cell to view additional clarifying comments (red-triangle)

- Tab 1 (Overall Cap Rating with Tip)- Shows 7 process areas at a high level
 - The model has 4 capability levels (0- Incomplete, 1-Performed, 2-Managed, 3-Defined).
- Tab 2 (Specific Goals by Process) – Shows the 7 process areas and all the specific goals defined for each process.

Round One Questionnaire for Delphi Group

SURVEY INSTRUCTIONS

1. Please read the following instructions before filling out this questionnaire. This questionnaire consists of open-ended questions.
2. Each of the open-ended questions has space provided for your reply. If there is insufficient room, continue to type and I will take care of any formatting problems when I receive the forms.
3. Specific responses of each respondent will be treated **anonymously**.
4. Please fill out “Participant Information” section below. No identify information will be in the final product, this information will be aggregated together to represent the respondents. For example, 5 members from the DIB, 1 member from academia, 3 members from DoD, etc. participated in a Delphi Study.
5. Please save the completed questionnaire as an MS Word document and e-mail it back to me at justin.swartzmiller@afit.af.mil

Participant Name _____
Participant Organization/Office Symbol _____

Appendix B – Proposed Cybersecurity Model Round One Overall Model

	A	B	C	D	E	F	G	H	I
1	Capability Level Ratings Overlaid on Targeted Improvement Profile								
2									
3	ASSET DEFINITION AND MANAGEMENT (ADM)								
4									
5	INCIDENT MANAGEMENT AND CONTROL (IMC)								
6									
7	KNOWLEDGE AND INFORMATION MANAGEMENT (KIM)								
8									
9	MONITORING (MON)								
10									
11	RISK MANAGEMENT (RISK)								
12									
13	TECHNOLOGY MANAGEMENT (TM)								
14									
15	VULNERABILITY ANALYSIS AND RESOLUTION (VAR)								
16		0	1	2	3				
17									
18									
19	CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience.								
20									
21									

Levels Defined

0	Incomplete
1	Performed
2	Managed
3	Defined

	A	B	C	D	E	F	G	H
1	ASSET DEFINITION AND MANAGEMENT (ADM)							
2	ADM:SG1 Establish Organizational Assets						<u>Legend</u> SG= Specific Goal SP= Specific Practice	
3	ADM:SG1.SP1 Inventory Assets							
4	ADM:SG1.SP2 Establish a Common Understanding							
5	ADM:SG1.SP3 Establish Ownership and Custodianship							
6	ADM:SG2 Establish the Relationship Between Assets and Services							
7	ADM:SG2.SP1 Associate Assets with Services							
8	ADM:SG2.SP2 Analyze Asset-Service Dependencies							
9	ADM:SG3 Manage Assets							
10	ADM:SG3.SP1 Identify Change Criteria							
11	ADM:SG3.SP2 Maintain Changes to Assets and Inventory							
12								
13	INCIDENT MANAGEMENT AND CONTROL (IMC)							
14	IMC:SG1 Establish the Incident Management and Control Process							
15	IMC:SG1.SP1 Plan for Incident Management							
16	IMC:SG1.SP2 Assign Staff to the Incident Management Plan							
17	IMC:SG2 Detect Events							
18	IMC:SG2.SP1 Detect and Report Events							
19	IMC:SG2.SP2 Log and Track Events							
20	IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence							
21	IMC:SG2.SP4 Analyze and Triage Events							
22	IMC:SG3 Declare Incidents							
23	IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria							
24	IMC:SG3.SP2 Analyze Incidents							
25	IMC:SG4 Respond to and Recover from Incidents							
26	IMC:SG4.SP1 Escalate Incidents							
27	IMC:SG4.SP2 Develop Incident Response							
28	IMC:SG4.SP3 Communicate Incidents							
29	IMC:SG4.SP4 Close Incidents							
30	IMC:SG5 Establish Incident Learning							
31	IMC:SG5.SP1 Perform Post-Incident Review							
32	IMC:SG5.SP2 Integrate with the Problem Management Process							
33	IMC:SG5.SP3 Translate Experience to Strategy							
34		0	1	2	3			
35	KNOWLEDGE AND INFORMATION MANAGEMENT (KIM)							
36	KIM:SG1 Establish and Prioritize Information Assets							
37	KIM:SG1.SP1 Prioritize Information Assets							
38	KIM:SG1.SP2 Categorize Information Assets							
39	KIM:SG2 Protect Information Assets							
40	KIM:SG2.SP1 Assign Resilience Requirements to Information Assets							
41	KIM:SG2.SP2 Establish and Implement Controls							
42	KIM:SG3 Manage Information Asset Risk							
43	KIM:SG3.SP1 Identify and Assess Information Asset Risk							
44	KIM:SG3.SP2 Mitigate Information Asset Risk							
45	KIM:SG4 Manage Information Asset Confidentiality and Privacy							
46	KIM:SG4.SP1 Encrypt High-Value Information							
47	KIM:SG4.SP2 Control Access to Information Assets							
48	KIM:SG4.SP3 Control Information Asset Disposition							
49	KIM:SG5 Manage Information Asset Integrity							
50	KIM:SG5.SP1 Control Modification of Information Assets							
51	KIM:SG5.SP2 Manage Information Asset Configuration							
52	KIM:SG5.SP3 Verify Validity of Information							
53	KIM:SG6 Manage Information Asset Availability							
54	KIM:SG6.SP1 Perform Information Duplication and Retention							
55	KIM:SG6.SP2 Manage Organizational Knowledge							

	A	B	C	D	E	F	G
56							
57	MONITORING (MON)						
58	MON:SG1 Establish and Maintain a Monitoring Program						
59	MON:SG1.SP1 Establish a Monitoring Program						
60	MON:SG1.SP2 Identify Stakeholders						
61	MON:SG1.SP3 Establish Monitoring Requirements						
62	MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements						
63	MON:SG2 Perform Monitoring						
64	MON:SG2.SP1 Establish and Maintain Monitoring Infrastructure						
65	MON:SG2.SP2 Establish Collection Standards and Guidelines						
66	MON:SG2.SP3 Collect and Record Information						
67	MON:SG2.SP4 Distribute Information						
68		0	1	2	3		
69	RISK MANAGEMENT (RISK)						
70	RISK:SG1 Prepare for Risk Management						
71	RISK:SG1.SP1 Determine Risk Sources and Categories						
72	RISK:SG1.SP2 Establish an Operational Risk Management Strategy						
73	RISK:SG2 Establish Risk Parameters and Focus						
74	RISK:SG2.SP1 Define Risk Parameters						
75	RISK:SG2.SP2 Establish Risk Measurement Criteria						
76	RISK:SG3 Identify Risk						
77	RISK:SG3.SP1 Identify Asset-Level Risks						
78	RISK:SG3.SP2 Identify Service-Level Risks						
79	RISK:SG4 Analyze Risk						
80	RISK:SG4.SP1 Evaluate Risk						
81	RISK:SG4.SP2 Categorize and Prioritize Risk						
82	RISK:SG4.SP3 Assign Risk Disposition						
83	RISK:SG5 Mitigate and Control Risk						
84	RISK:SG5.SP1 Develop Risk Mitigation Plans						
85	RISK:SG5.SP2 Implement Risk Strategies						
86	RISK:SG6 Use Risk Information to Manage Resilience						
87	RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services						
88	RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services						
89							

90	TECHNOLOGY MANAGEMENT (TM)				
91	TM:SG1 Establish and Prioritize Technology Assets				
92	TM:SG1.SP1 Prioritize Technology Assets				
93	TM:SG1.SP2 Establish Resilience-Focused Technology Assets				
94	TM:SG2 Protect Technology Assets				
95	TM:SG2.SP1 Assign Resilience Requirements to Technology Assets				
96	TM:SG2.SP2 Establish and Implement Controls				
97	TM:SG3 Manage Technology Asset Risk				
98	TM:SG3.SP1 Identify and Assess Technology Asset Risk				
99	TM:SG3.SP2 Mitigate Technology Risk				
100		0	1	2	3
101	TECHNOLOGY MANAGEMENT (TM) CONTINUED				
102	TM:SG4 Manage Technology Asset Integrity				
103	TM:SG4.SP1 Control Access to Technology Assets				
104	TM:SG4.SP2 Perform Configuration Management				
105	TM:SG4.SP3 Perform Change Control and Management				
106	TM:SG4.SP4 Perform Release Management				
107	TM:SG5 Manage Technology Asset Availability				
108	TM:SG5.SP1 Perform Planning to Sustain Technology Assets				
109	TM:SG5.SP2 Manage Technology Asset Maintenance				
110	TM:SG5.SP3 Manage Technology Capacity				
111	TM:SG5.SP4 Manage Technology Interoperability				
112					
113	VULNERABILITY ANALYSIS AND RESOLUTION (VAR)				
114	VAR:SG1 Prepare for Vulnerability Analysis and Resolution				
115	VAR:SG1.SP1 Establish Scope				
116	VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy				
117	VAR:SG2 Identify and Analyze Vulnerabilities				
118	VAR:SG2.SP1 Identify Sources of Vulnerability Information				
119	VAR:SG2.SP2 Discover Vulnerabilities				
120	VAR:SG2.SP3 Analyze Vulnerabilities				
121	VAR:SG3 Manage Exposure to Vulnerabilities				
122	VAR:SG3.SP1 Manage Exposure to Vulnerabilities				
123	VAR:SG4 Identify Root Causes				
124	VAR:SG4.SP1 Perform Root-Cause Analysis				
125		0	1	2	3
126	CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience.				

Appendix C – Delphi Questionnaire Round One

1. In a sentence or two please, describe your experience with Cybersecurity and Information Security.
2. What do you think are the top problems your organization faces in providing Cybersecurity?
3. Do you see any problems with requiring <u>all</u> (smaller-larger) members of the DIB to secure their respective Cyberspace (networks computer systems and infrastructure) under their control?
4. There are frequent reports of cyber intrusions (penetrations into a network) which has resulted in the loss of sensitive information and intellectual property. When this happens to the DoD and/or a DIB member, what effects could it have on your organization?
5. Please explain, why or why not, implementing a Cyberspace maturity model could help the DIB better focus their efforts in defending their Cyberspace.
6. I've introduced the CERT-Resilience Management Model as a way to access Cyberspace security, was it clear with its intent? What are its strengths? What are its weaknesses?
7. Describe how successful the proposed Cyberspace Maturity Model captures the vital processes that should be evaluated in determining an organizations Cyberspace security.

8. List and describe any processes you would include or delete from the proposed Cyberspace Maturity Model?
9. What recommendation would you make to make this model more useful?
10. Are in favor of having this Cyberspace Maturity Model in place to appraise DIB members in measuring their Cyberspace security? Please list your supporting reasons.
11. Please provide any additional comments that you believe will be helpful to this study.

Thank you for your valuable time.

Appendix D - Delphi Group Instructions Round Two

What is the purpose of round two?

The Delphi Technique is performed in a series of rounds. This iterative process of rounds and analysis continues until a consensus or stabilization point has been reached.

How does the panel reach consensus?

This questionnaire contains both the panel's answers from round one and follow-up questions that will help the panel reach a consensus. The question makeup is as follows:

- Original question (round one)
- Analyzed answer from the panel
 - Follow-up question for round two

What changes were made to the Cyberspace Maturity Model?

Per the panels recommendations a review was done to ensure that the proposed Cyberspace Maturity Model includes some of the well recognized codes of practice such as: *Information Technology Infrastructure Library* (ITIL), information security standards published by the *International Organization for Standardization* (ISO) and the *International Electrotechnical Commission* (IEC), 27000, *Control Objectives for Information and related Technology* (COBIT), and *National Institute for Standards and Technology* (NIST).

Two new processes areas were added to the Cyberspace Maturity Model: Organizational Training & Awareness (OTA) and Resilient Technical Solution Engineering (RTSE) plus the monitoring and incident management & control processes were expanded.

Please refer to the attached capability model when responding to the questions:

The updated Cyberspace Maturity Model for the DIB can be found at the attached Excel spreadsheet:

- * Roll mouse over each cell to view additional clarifying comments (red-triangle)
- Tab 1 (Overall Cap Rating with Tip)- Shows 9 process areas at a high level
 - The model has 4 capability levels (0- Incomplete, 1-Performed, 2-Managed, 3-Defined).
- Tab 2 (Specific Goals by Process) – Shows the 9 process areas and all the specific goals defined for each process.
- Updates (additions) are highlighted

SURVEY INSTRUCTIONS

Each of the open-ended questions has space provided for your reply. If there is insufficient room, continue to type and I will take care of any formatting problems when I receive the forms.

Specific responses of each respondent will be treated anonymously.

Please save the completed questionnaire as an MS Word document and return it to me by **23 April 2012** at justin.swartzmiller@afit.af.mil

Appendix E - Modified Cybersecurity Model Round Two

	A	B	C	D	E	F	G	H	I
1	Capability Level Ratings Overlaid on Targeted Improvement Profile								
2									
3	ASSET DEFINITION AND MANAGEMENT (ADM)								
4									
5	INCIDENT MANAGEMENT AND CONTROL (IMC)								
6									
7	KNOWLEDGE AND INFORMATION MANAGEMENT (KIM)								
8									
9	MONITORING (MON)								
10									
11	ORGANIZATIONAL TRAINING AND AWARENESS (OTA)								
12									
13	RESILIENT TECHNICAL SOLUTION ENGINEERING (RTSE)								
14									
15	RISK MANAGEMENT (RISK)								
16									
17	TECHNOLOGY MANAGEMENT (TM)								
18									
19	VULNERABILITY ANALYSIS AND RESOLUTION (VAR)								
20		0	1	2	3				
21									
22									
23	CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience.								
24									
25									

Levels Defined

0	Incomplete
1	Performed
2	Managed
3	Defined

	A	B	C	D	E	F	G
1	ASSET DEFINITION AND MANAGEMENT (ADM)						
2	ADM:SG1 Establish Organizational Assets	Legend SG= Specific Goal SP= Specific Practice					
3	ADM:SG1.SP1 Inventory Assets						
4	ADM:SG1.SP2 Establish a Common Understanding						
5	ADM:SG1.SP3 Establish Ownership and Custodianship						
6	ADM:SG2 Establish the Relationship Between Assets and Services						
7	ADM:SG2.SP1 Associate Assets with Services						
8	ADM:SG2.SP2 Analyze Asset-Service Dependencies						
9	ADM:SG3 Manage Assets						
10	ADM:SG3.SP1 Identify Change Criteria						
11	ADM:SG3.SP2 Maintain Changes to Assets and Inventory						
12							
13	INCIDENT MANAGEMENT AND CONTROL (IMC)						
14	IMC:SG1 Establish the Incident Management and Control Process						
15	IMC:SG1.SP1 Plan for Incident Management						
16	IMC:SG1.SP2 Assign Staff to the Incident Management Plan						
17	IMC:SG2 Detect Events						
18	IMC:SG2.SP1 Detect and Report Events						
19	IMC:SG2.SP2 Log and Track Events						
20	IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence						
21	IMC:SG2.SP4 Analyze and Triage Events						
22	IMC:SG3 Declare Incidents						
23	IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria						
24	IMC:SG3.SP2 Analyze Incidents						
25	IMC:SG4 Respond to and Recover from Incidents						
26	IMC:SG4.SP1 Escalate Incidents						
27	IMC:SG4.SP2 Develop Incident Response						
28	IMC:SG4.SP3 Communicate Incidents						
29	IMC:SG4.SP4 Share Incident Information with Outside Partners						
30	IMC:SG4.SP5 Close Incidents						
31	IMC:SG5 Establish Incident Learning						
32	IMC:SG5.SP1 Perform Post-Incident Review						
33	IMC:SG5.SP2 Integrate with the Problem Management Process						
34	IMC:SG5.SP3 Translate Experience to Strategy						
35		0	1	2	3		
36	KNOWLEDGE AND INFORMATION MANAGEMENT (KIM)						
37	KIM:SG1 Establish and Prioritize Information Assets						
38	KIM:SG1.SP1 Prioritize Information Assets						
39	KIM:SG1.SP2 Categorize Information Assets						
40	KIM:SG2 Protect Information Assets						
41	KIM:SG2.SP1 Assign Resilience Requirements to Information Assets						
42	KIM:SG2.SP2 Establish and Implement Controls						
43	KIM:SG3 Manage Information Asset Risk						
44	KIM:SG3.SP1 Identify and Assess Information Asset Risk						
45	KIM:SG3.SP2 Mitigate Information Asset Risk						
46	KIM:SG4 Manage Information Asset Confidentiality and Privacy						
47	KIM:SG4.SP1 Encrypt High-Value Information						
48	KIM:SG4.SP2 Control Access to Information Assets						
49	KIM:SG4.SP3 Control Information Asset Disposition						
50	KIM:SG5 Manage Information Asset Integrity						
51	KIM:SG5.SP1 Control Modification of Information Assets						
52	KIM:SG5.SP2 Manage Information Asset Configuration						
53	KIM:SG5.SP3 Verify Validity of Information						
54	KIM:SG6 Manage Information Asset Availability						
55	KIM:SG6.SP1 Perform Information Duplication and Retention						
56	KIM:SG6.SP2 Manage Organizational Knowledge						
57							

58	MONITORING (MON)				
59	MON:SG1 Establish and Maintain a Monitoring Program				
60	MON:SG1.SP1 Establish a Monitoring Program				
61	MON:SG1.SP2 Identify Stakeholders				
62	MON:SG1.SP3 Establish Monitoring Requirements				
63	MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements				
64	MON:SG2 Perform Monitoring				
65	MON:SG2.SP1 Establish and Maintain Monitoring Infrastructure				
66	MON:SG2.SP2 Establish Collection Standards and Guidelines				
67	MON:SG2.SP3 Collect and Record Information				
68	MON:SG2.SP4 Demonstrate Process of Detecting Signatures				
69	MON:SG2.SP5 Distribute Information				
70		0	1	2	3
71	ORGANIZATIONAL TRAINING AND AWARENESS (OTA)				
72	OTA:SG1 Establish Awareness Program				
73	OTA:SG1.SP1 Establish Awareness Needs				
74	OTA:SG1.SP2 Establish Awareness Plan				
75	OTA:SG1.SP3 Establish Awareness Delivery Capability				
76	OTA:SG2 Conduct Awareness Activities				
77	OTA:SG2.SP1 Perform Awareness Activities				
78	OTA:SG2.SP2 Establish Awareness Records				
79	OTA:SG2.SP3 Assess Awareness Program Effectiveness				
80	OTA:SG3 Establish Training Capability				
81	OTA:SG3.SP1 Establish Training Needs				
82	OTA:SG3.SP2 Establish Training Plan				
83	OTA:SG3.SP3 Establish Training Capability				
84	OTA:SG4 Conduct Training				
85	OTA:SG4.SP1 Deliver Training				
86	OTA:SG4.SP2 Establish Training Records				
87	OTA:SG4.SP3 Assess Training Effectiveness				
88		0	1	2	3
89	RESILIENT TECHNICAL SOLUTION ENGINEERING (RTSE)				
90	RTSE:SG1 Establish Guidelines for Resilient Technical Solution Development				
91	RTSE:SG1.SP1 Identify General Guidelines				
92	RTSE:SG1.SP2 Identify Requirements Guidelines				
93	RTSE:SG1.SP3 Identify Architecture and Design Guidelines				
94	RTSE:SG1.SP4 Identify Implementation Guidelines				
95	RTSE:SG1.SP5 Identify Assembly and Integration Guidelines				
96	RTSE:SG2 Develop Resilient Technical Solution Development Plans				
97	RTSE:SG2.SP1 Select and Tailor Guidelines				
98	RTSE:SG2.SP2 Integrate Selected Guidelines with a Defined Software and System Development Process				
99	RTSE:SG3 Execute the Plan				
100	RTSE:SG3.SP1 Monitor Execution of the Development Plan				
101	RTSE:SG3.SP2 Release Resilient Technical Solutions into Production				
102		0	1	2	3
103	RISK MANAGEMENT (RISK)				
104	RISK:SG1 Prepare for Risk Management				
105	RISK:SG1.SP1 Determine Risk Sources and Categories				
106	RISK:SG1.SP2 Establish an Operational Risk Management Strategy				
107	RISK:SG2 Establish Risk Parameters and Focus				
108	RISK:SG2.SP1 Define Risk Parameters				
109	RISK:SG2.SP2 Establish Risk Measurement Criteria				
110	RISK:SG3 Identify Risk				
111	RISK:SG3.SP1 Identify Asset-Level Risks				
112	RISK:SG3.SP2 Identify Service-Level Risks				
113	RISK:SG4 Analyze Risk				
114	RISK:SG4.SP1 Evaluate Risk				
115	RISK:SG4.SP2 Categorize and Prioritize Risk				
116	RISK:SG4.SP3 Assign Risk Disposition				
117	RISK:SG5 Mitigate and Control Risk				
118	RISK:SG5.SP1 Develop Risk Mitigation Plans				
119	RISK:SG5.SP2 Implement Risk Strategies				
120	RISK:SG6 Use Risk Information to Manage Resilience				
121	RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services				
122	RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services				
123					

Appendix F - Delphi Questionnaire Round Two

1. In a sentence or two please, describe your experience with Cybersecurity and Information Security.

Our Panel Statistics:

- Panel Makeup: 3 DIB contractors, 2 sitting Unit Commanders, 1 COCOM, 1 Acquisition, 1 Academic, 1 Security Threat Consultant, and 1 Cyber Crime Specialist (10 Members)
- 9 out of 10 members were able to respond in round one
- Each member has a minimum of 10 years experience in Information Security/Cyber Field
- 3 members hold PhD's in a Cyber discipline
- All members are currently working in the Cyber realm, thus are maintaining currency

➤ Please comment if the anonymous categories in Panel Makeup do not accurately represent you: _____

2. What do you think are the top problems your organization faces in providing Cybersecurity?

The group responses were focused on their respective organizations as requested however some problems were identified by more than one member.

- 4 members specifically mentioned training of personnel or lack of real cyber expertise
- 4 members specifically mentioned Management/Management support/Bureaucracy of Corporation/How Organized
- 3 members specifically identified: limited resources/current budget level/budgetary priority
- Other identified problem areas:
 - Involving security from project birth
 - Getting programmers to understand security, vulnerabilities, and exploitations
 - Penetration testing with techniques of hackers
 - Sharing of incident information; openly
 - Testing stability and security of unique software development efforts
 - Finding security incidents even while monitoring
 - Maintaining fully patches systems; patches continuously coming out

- Given the overview of top problems within your respective organizations, are you largely in agreement with the problems identified above? Do you have any additional comments?

3. Do you see any problems with requiring all (smaller-larger) members of the DIB to secure their respective Cyberspace (networks computer systems and infrastructure) under their control?

- 4 members responded no.
- 5 members responded yes. Of the yes's:
 - 3 expressed concerns over resources of smaller companies
 - 1 stated enforcement could be an issue
 - 1 stated there is no way to be 100% secure, especially against a motivated attacker

Additional Information for the round two question;

- If a Cyberspace maturity model was approved and implemented; future request for proposals (RFP) could include a provision such as: demonstration of having achieved a capability level 2 within the Cyberspace maturity model is required or even highly desired. (Much like was used with software acquisition). This could incentivize all DIB members; although this would drive contract prices up it may be worthwhile.
 - Since the Cyberspace maturity model is based on the CERT-RMM there is an established formalized appraisal process with appraisers already trained and in place. The presented Cyberspace maturity model is a more focused model but the appraisers and appraisal process are unchanged.
- Please comment further given the additional information; do you see any problems with requiring all members of the DIB to secure their respective Cyberspace?

4. There are frequent reports of cyber intrusions (penetrations into a network) which has resulted in the loss of sensitive information and intellectual property. When this happens to the DoD and/or a DIB member, what effects could it have on your organization?

The group responses were focused on their respective organizations as requested. I've paraphrased most of the responses below:

- Significant financial and liability impact
 - Large impact on national security via the long term “bleeding”
 - Decision makers have near zero visibility into after effects/ongoing risks that intrusions present to mission capabilities
 - When media reports intrusions, attackers change tactics which makes future detection more difficult
 - Compromising U.S. weapon system during development
 - Grave effects-DIB partners may contain system vulnerabilities that could aide the enemy
 - Affects people through loss of PII (personal identifiable information)
 - Affects DoD's image to U.S. citizens
- Please rank the **top 3** affects the loss of sensitive information and intellectual property could have taking the entire DIB (both DoD and DIB contractors) into context.

1)

2)

3)

5. Please explain, why or why not, implementing a Cyberspace maturity model could help the DIB better focus their efforts in defending their Cyberspace.

All members responded that implementing a Cyberspace maturity model could help the DIB focus their efforts. The below responses define why a Cyberspace maturity model could help:

- Provides a framework for prioritizing actions, improvements, comparison benchmarks and goals
 - Provides a common framework for communication exchange and requirements
 - Educate management on the importance of securing the network
 - Provides a way for government contract managers to choose the more secure companies (on paper)
 - Improve the security posture and help understand the network “hygiene” of organizations which work together
 - Could give them a plan to improve their security posture
 - Identifies similar goals organizations could work towards
- Given that the panel stated implementing a Cyberspace maturity model could help the DIB focus their efforts, are you in favor of describing why it would help as:

A Cyberspace maturity model could help the DIB better focus their efforts in defending their Cyberspace by providing:

- A common starting point
 - A framework for prioritizing actions
 - A way to define what improvement means to an organization
 - And it can be used as a benchmark for comparison
- Yes or no?
- If no, what other statement(s) should be included?

6. I've introduced the CERT-Resilience Management Model as a way to access Cyberspace security, was its intent clear?

All members responded yes, the intent was clear.

What are its strengths?

- The below strengths were reported; please review them and mark your concurrence in the appropriate column.

Strength	Agree	Disagree
Operational Resilience		
Incremental Process Improvement		
Intended Results		
Common Framework for Evaluating Processes		
Coverage of General Principles for Establishing Security Processes		
Common Framework to help improve Security Capability		
Focuses on where Vulnerabilities exist		
Model builds on Established Models that may be familiar to Org's		
Seven Processes and Associated SP's thoroughly cover main ideas in the Cyber Security Space		

What are its weaknesses?

- The below weaknesses were reported; please review them and mark your concurrence in the appropriate column.

Weakness	Agree	Disagree
Lack of details		
No Maturity Levels		
Hard to Address Deployment Effectiveness in a Real Environment		
Does not address Abilities of People (skill, training, experience)		
Model too focused, include: Education, Training and Technology		
Lack of Definition of SPs		
The Rating/Scoring System		

7. Describe how successful the proposed Cyberspace Maturity Model captures the vital processes that should be evaluated in determining an organizations Cyberspace security.

Overall the panel favorably responded that the proposed Cyberspace Maturity Model captures the vital processes.

- The caveats provided by the members are incorporated into question 8.

8. List and describe any processes you would include or delete from the proposed Cyberspace Maturity Model?

The panel did not identify any areas that should be deleted.

The panel suggested including the following additions, however these are currently embedded in the identified processes:

- Forensics→ **Incident Management And Control (IMC)**
- Audits→ **Incident Management And Control (IMC)**
- Tools and Technology→ **Technology Management (TM)**

The panel suggested including the following additions, these processes where added and are highlighted in the model:

- Penetration Testing → **Resilient Technical Solution Engineering (RTSE)**
- Human Factors (abilities of people-skill sets, training, job knowledge, experience, etc)
→ **Organizational Training And Awareness (OTA)**
- Expand the monitoring section → Added detecting of signatures
- Expand incident management & control → Added forensics and share incident information

Please refer to the updated Cyberspace Maturity Model and review the highlighted areas.

- Do you feel the proposed Cyberspace Maturity Model captures the vital processes that should be evaluated in determining an organizations Cyberspace security?
- If no, please list proposed processes.

9. What recommendation would you make to make this model more useful?

- The panel identified numerous recommendations that could make the introduced model more useful; please review them and mark your concurrence in the appropriate column.

Recommendations	Agree	Disagree
Identify more specific controls for auditing capabilities		
Combine asset management and technology management		
Introduce Associated Scoring- would allow other org's to understand where accessed org's- scoring as is limited to 'does' or 'does not'		
Reorganize sections to follow a standard or development lifecycle		
Include context relating to cost with implementation and maintenance of maturity level (Beneficial to both large and small org's)		

10. Are in favor of having this Cyberspace Maturity Model in place to appraise DIB members in measuring their Cyberspace security?

- 6 members responded yes.
- 3 members responded no. The concerns/reservations raised were:
 - Model could become compliance based as opposed to addressing real issues surrounding cyber security
 - This CMM could end up being a audit or checkbox used to win contracts
 - Scoring does not provide enough granularity

Additional Information for the round two question;

- The proposed Cyberspace Maturity Model is based on the CERT-RMM which focuses on the processes of an organization and ultimately their operational resilience in those processes. It is a shift from the a Capability Maturity Model (CMM) as in the Cyberspace Maturity Model organizations are assessed by reaching a capability level and within each level how they are improving; thus no maturity is ever achieved.
 - Scoring detail was purposely omitted to focus on which processes to include within the model. However, to reach a particular capability level, an organization must satisfy all of the appropriate goals (Specific Goals and Specific Processes) of the process areas. An organization would receive the lowest level rating of which they satisfied all goals. There is currently no staged representation scoring in the CERT-RMM, but it can be viewed as those organizations that reach a higher capability levels in each process area are exhibiting a higher degree of (maturity).
- Please comment further given the additional information; are in favor of having this Cyberspace Maturity Model in place to appraise DIB members in measuring their Cyberspace security?

Thank you for your valuable time.

Bibliography

- Alperovitch, D. (2011). *Revealed: Operation Shady RAT* (p. 2). McAfee. Retrieved from <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>
- Caralli, Richard A., Julia H. Allen and David W. White (2011). *CERT Resilience Management Model, A Maturity Model for Managing Operational Resilience*. Boston: Pearson Education, Inc, 2011.
- Chichonski, Paul, Tom Millar, Tim Grance and Karen Scarfone (2012). Computer Security Incident Handling Guide (Draft), *National Institute of Standards and Technology*. Gaithersburg, MD: U.S. Department of Commerce, January 2012.
- Clatyon, Mark J. "Delphi: A Technique to Harness Expert Opinion for Critical Decision-Making Tasks in Education", *Education Psychology*, 17:4, Dec 1997.
- Dalkey, N. C., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science*, 9 (3), 458-467.
- Defense Security Service (2009). *A Trend Analysis of Reporting from Defense Industry 2008*. Report. Washington: GPO, 16 January 2009.
- Department of Defense (2010). *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*. DOD Instruction 5205.13. Washington: GPO, 29 January 2010.
- Department of Defense (2011). *Department of Defense Dictionary of Military and Associated Terms*. JP 1-02. Washington: GPO, 8 Nov 2010, Amended 15 May 2011.
- Department of Defense (2011). *National Industrial Security Program (NISP) Fact Sheet*. Washington: Defense Security Service, (December 2011)
http://www.dss.mil/about_dss/fact_sheets/nisp_faqsheet.html
- Department of Defense (2011). *Strategy for Operating in Cyberspace*. Washington: GPO, July 2011.
- Department of Defense (2012). Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program. 9 January 2012 <http://dibnet.dod.mil/>
- Department of Homeland Security (2008). Fact Sheet: *Protecting Our Federal Networks Against Cyber Attacks*. Washington: Homeland Security Digital Library, 8 April 2008
<http://www.hsdl.org/?view&did=486707>.
- Department of Homeland Security (2008). Project 12 Report: *Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnerships*. Washington: GPO, November 2008.

- Department of Homeland Security (2012). *Joint Cybersecurity Services Pilot (JCSP)*. Washington: GPO, January 13, 2012.
- Department of Justice (2004). *Task Force on Intellectual Property*. Report. Washington: GPO, October 2004.
- Erffmeyer, R. C., Erffmeyer, E. S., and Lane, I.M., (1986). The Delphi Technique: An Empirical Evaluation of the Optimal Number of Rounds. *Groups and Organization Studies* 11 (1-2), 120-128 (1986).
- Ewing, Philip (2012). "Has the 'Cyber Pearl Harbor' already happened?" *DoD Buzz: Online Defense and Acquisition Journal*, 26 March 2012
<http://www.dodbuzz.com/2012/03/26/has-the-cyber-pearl-harbor-already-happened/>
- Fisher, Dennis (2012). White House Launches Electric Industry Security Maturity Model Program. *The Kaspersky Lab Security News Service*, January 10, 2012.
http://threatpost.com/en_us/blogs/white-house-launches-electric-industry-security-maturity-model-program-011012.
- Hsu, Chia-Chien and Brian A. Sandford (2007). *The Delphi Technique: Making Sense of Consensus*. Practical Assessment, Research & Evaluation Journal, 12 (10): 1-8 (August 2007) <http://pareonline.net/pdf/v12n10.pdf>
- Kanellos, Michael (2003). *Moore's Law to roll on for another decade*. CNET News, 10 Feb 2003 <http://news.cnet.com/2100-1001-984051.html>
- Linstone, H. A., & Turoff, M. (1975). Introduction. In H. A. Linstone, & M. Turoff (Eds.) *The Delphi method: Techniques and applications* (pp. 3-12). Reading, MA: Addison-Wesley Publishing Company.
- Ludwig, B. G. (1994). *Internationalizing Extension: An exploration of the characteristics evident in a state university Extension system that achieves internationalization*. Unpublished doctoral dissertation, The Ohio State University, Columbus.
- Magnuson, Stew (2011). Defense Department Partners with Industry to Stem Staggering Cybertheft Losses, *National Defense Magazine*, December 2011.
- McConnell, Mike, Michael Chertoff and William Lynn (2012). China's Cyber Thievery is National Policy—And must be Challenged. *Wall Street Journal*, January 27, 2012.
- Nakashima, Ellen (2008). Bush Order Expands Network Monitoring. *The Washington Post*, January 26, 2008.
- National Counterintelligence Center (1995). *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*. Washington: GPO, 1995.

- National Counterintelligence Center (1996). *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*. Washington: GPO, 1996.
- National Counterintelligence Center (2001). *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*. Washington: GPO, 2001.
- National Counterintelligence Center (2005). *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*. Washington: GPO, 2005.
- Obama, Barak (2009). *The Comprehensive National Cybersecurity Initiative (CNCI)*. Washington: White House, 2009.
- Obama, Barak (2009). *Cyberspace Policy Review*. Washington: White House, May 2009.
- Obama, Barak (2011). *International Strategy For Cyberspace May 2011*. Washington: White House, 2011.
- Office of the National Counterintelligence Executive (2011). *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011. Washington: GPO, October 2011.
- Pellerin, Cheryl (2011). *DOD, Partners Better Prepared for Cyber Attacks*. American Forces Press Service. Washington, 18 Oct 2011
<http://www.defense.gov/news/newsarticle.aspx?id=65709>
- Rowe, G., Wright, G., and Bolger, F., (1991) Delphi: A Reevaluation of Research and Theory, *Technological Forecasting and Social Change* 39, 235-251 (1991).
- United States Government Accounting Office (2011). *Defense Department Cyber Efforts*. GAO-11-75. Washington: GAO, July 2011.
- United States House of Representatives (2012). *18 USC Sec 1831* (January 2012)
<http://uscode.house.gov/download/pls/18C90.txt>
- United States House of Representatives (2012). *18 USC Sec 1832*(January 2012)
<http://uscode.house.gov/download/pls/18C90.txt>
- Verizon Risk Team (2012). Data Breach Investigations Report. Verizon Business, March 2012. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
- White, Gregory B. (2011) “The Community Cyber Security Maturity Model,” *Proceeding of the IEEE 11th Conference on the Technologies for Homeland Security (HST)*. 173-178. New York: IEEE Press, 2011.

Vita

Major Justin Swartzmiller graduated from Southern Local High School in Salineville, Ohio in June 1989. He entered the Air Force in March 1990 and attended basic training. He spent the next 8 years working with the Traffic Management Office (TMO) at several bases and deployed locations, where he attained the rank of Staff Sergeant. Major Swartzmiller has an Associate of Science from the Community College of the Air Force in Transportation. He received his Bachelor of Science Degree in Computer Information Systems from Chapman University, graduating in 1997. He separated from active duty and was accepted into the Reserve Officer Training Corps (ROTC) at the University of New Mexico in January 1998. While attending ROTC, Major Swartzmiller pursued his Masters degree. He graduated with a Masters of Business Administration (MBA) and received his Commission in July 1999.

Upon his Commissioning, Major Swartzmiller was selected to be a Logistics Readiness Officer. His first assignment was at Little Rock AFB as the Chief of the 463rd Airlift Group Logistics Plans in September 1999. In May 2002, he was assigned to the Air Force Research Laboratory, Human Effectiveness Directorate, Logistics Research Branch at Wright-Patterson AFB, Ohio where he served as a Logistics Research Officer. While stationed at Wright-Patterson AFB, he deployed to Istres AB, France where he served as the Chief of Logistics for three months. He was competitively selected to serve as the Executive Officer for the Chief Technologist of the Air Force Research Laboratory in April 2004 and served in the position until November 2005. He attended Squadron Officer School at Maxwell AFB, Alabama in 2005 where his flight earned the Coach Ray

Eliot award and was ranked #1 of 34 flights for competitive field leadership. In November 2005, he was assigned to Hickam AFB, Hawaii as the 15th Logistics Readiness Squadron, Installation Readiness Flight Commander. He was promoted to be the Director of Operations of the 15th Logistics Readiness Squadron during January 2007. While stationed at Hickam AFB, he deployed to Kuwait City International Airport, Kuwait as the Assistant Director of Operations for four months in 2007. In September 2008, he was assigned to Camp H. M. Smith, Hawaii as the Deputy Director of the PACOM Deployment Distribution Operations Center (DDOC). He was competitively selected, in February 2010, to serve as the Country Director for Vietnam, Cambodia, and Laos. In May 2011, he entered the Intermediate Development Education (IDE) Cyber Warfare program of the Department of Electrical and Computer Engineering at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio. Upon graduation, Major Swartzmiller will be assigned to the United States Military Training Mission (USMTM), Riyadh, Saudi Arabia.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 074-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>					
1. REPORT DATE (DD-MM-YYYY) 14-06-2012		2. REPORT TYPE Graduate Research Project		3. DATES COVERED (From – To) May 2011 –June 2012	
4. TITLE AND SUBTITLE Securing the next ripple in Information Security: The Defense Industrial Base (DIB)				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Swartzmiller, Justin, W., Major, USAF				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way, Building 640 WPAFB OH 45433-7765				8. PERFORMING ORGANIZATION REPORT NUMBER AFIT/ICW/ENV/12-J02	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) DoD Cyber Crime Center (DC3) (POC: Steven D. Shirley, SES, DAF) 911 Elkridge Landing Rd Airport Sq 11, Ste 200 Linthicum, MD 21090				10. SPONSOR/MONITOR'S ACRONYM(S) DC3	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.					
13. SUPPLEMENTARY NOTES This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.					
14. ABSTRACT America's one-time technological advantage is gone; much of its intellectual property secrets have been stolen. For sometime, our adversaries have been attacking the Department of Defense's (DoD) networks to obtain any sensitive information. Recently, attackers have expanded their attacking efforts, to include the Defense Industrial Base (DIB), due to DoD's increased network defenses. This research paper will answer the core issue of how to secure sensitive information within the DIB and determine if a Cybersecurity Maturity Model can be utilized to assess the level of security the DIB provides to sensitive unclassified DoD information? An initial Literature Review was conducted and the findings were used to develop a maturity model that may be used to enhance cybersecurity within the DIB. Next, a Delphi study was conducted to evaluate the proposed Cybersecurity Maturity Model methodology using four criteria: comprehensiveness, accuracy, completeness, and usefulness. The Delphi committee consisted of representatives from both the DoD and private sector; with each member's experience characterized as computer network attack, computer network exploitation or computer network defense. The findings of the Delphi committee support that a Cybersecurity Maturity Model can be developed successfully to better focus the DIB's efforts and demonstrate an organizations cyber security capability.					
15. SUBJECT TERMS Delphi technique, Cyberspace, Maturity Model, Defense Industrial Base (DIB), Information Security					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Alan R. Heminger, PhD (ENV)
U	U	U	UU	105	19b. TELEPHONE NUMBER (Include area code) (937)257-3636x4797; alan.heminger@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18